FOCUS FAMILY

ISO Conformity Profile

What Focus Family contributes to your certification – and what it does not

Software Notion · Kornblumenring 40 · 31600 Uchte · Germany · Product state 1.4.0 · Assessed 8 Nov 2026

Contents

1. **About this document**
   1. Why it exists
   2. What it explicitly is not
   3. Basis of assessment
2. **Executive summary**
   1. Overall picture
   2. Six key statements
3. **How standards and software relate**
   1. The organisation is certified, not the software
   2. What this means for your assessment
4. **Division of responsibility: vendor and operator**
5. **ISO/IEC 27001 – Information security management system**
   1. What the software provides
   2. What you must provide yourself
   3. Where it currently falls short
6. **ISO/IEC 27034 – Application security**
   1. What the standard is about
   2. What the software provides
   3. What you must provide yourself
   4. Where it currently falls short
7. **ISO/IEC 25010 – Software product quality**
   1. Functional suitability – met
   2. Performance efficiency – partial
   3. Compatibility – met
   4. Interaction capability – partial
   5. Reliability – met
   6. Security – met
   7. Maintainability – met
   8. Flexibility – met
   9. Safety – partial
8. **ISO/IEC 29147 and 30111 – Handling vulnerabilities**
   1. What they cover
   2. Current state
   3. What already works in practice
   4. What this means for you today
9. **Where Focus Family currently impedes your certification**
10. **Deliberate limits of the product**
11. **Data protection and openness**
    1. No vendor lock-in for your data
    2. Data protection as a product feature
    3. Where openness currently ends
12. **Open items and planned improvements**
13. **Evidence register**
14. **Questions you should be asking us**
15. **Contact and validity**

About this document

Why it exists

You are evaluating whether Focus Family can be deployed in your organisation. If your organisation runs an information security management system, is already certified to ISO/IEC 27001, or intends to become certified, you must be able to answer three questions for every application you deploy: **which security measures does the software provide, which must we provide ourselves, and where do gaps remain?**

This document answers exactly those three questions, for four standards:

Standard	Subject
ISO/IEC 27001:2022	Information security management system (ISMS)
ISO/IEC 27034	Application security
ISO/IEC 25010:2023	Software product quality
ISO/IEC 29147 / 30111	Vulnerability disclosure and handling

What it explicitly is not

This document is **not a certificate**, **not an assessment report by an accredited body**, and **not a warranty of conformity**. It is a vendor self-assessment produced by a structured review of the actual source code, the configuration and the documentation. You are free to challenge every statement in it — the section "Evidence register" names, for each claim, the artefact that substantiates it.

We follow one rule: **we would rather name an inconvenient gap than make an assurance that does not hold when it matters.** You will therefore find a substantial section describing what Focus Family **cannot** do, and where it currently **impedes** your certification.

Basis of assessment

Item	Value
Product state	1.4.0
Assessment date	8 November 2026 (version 1.4.0, build 26308)
Method	Source code review, configuration and deployment review, documentation reconciliation, test run
Depth	All security-relevant code paths of the server, the synchronisation layer and the encryption
Test evidence	6,243 tests: 6,229 passed, 14 skipped (environment-dependent), 0 failed; all seven test suites on the assessment date, the server and licensing suites against two PostgreSQL 17 instances including the upgrade test from version 1.0.0, with no database test skipped
Not assessed	Runtime behaviour of your specific installation, your operating environment, your organisational procedures

---

Executive summary

Overall picture

Standard	Maturity	Short assessment
ISO/IEC 27001	**supportive, strong**	The technical measures of Annex A are largely implemented and evidenced; of 66 addressable controls, 40 fully and 26 partially, none open. The software additionally generates compliance documents for you.
ISO/IEC 27034	**partial**	Every substantive element exists (requirements specification, threat model, controls, verification tests); control library and level of trust are not yet assembled in the form the standard expects. This is where the greatest short-term potential lies.
ISO/IEC 25010	**strong, three characteristics partial**	Six of nine quality characteristics are fully evidenced; performance efficiency, interaction capability and safety partially. The open point that matters most to you is **accessibility**: screen reader labels are complete and a statement exists, testing with real assistive technology is outstanding.
ISO/IEC 29147 / 30111	**in place, not yet exercised**	Reporting channel published and mailbox in place (`security.txt` , deadlines by severity), handling process with roles and deadlines described, reporting function in the admin panel, the app and the desktop. As no release has yet had to close a reported vulnerability, disclosure, advisory and post-release review are described but have never been carried out.

Six key statements

1. **Your data stays with you.** There is no vendor cloud. The server runs in your infrastructure, under your control, with your keys. The vendor has no access to your case data – neither technically nor by contractual design. Data leaves your installation for third-party systems only through interfaces that you set up yourself and that your data protection role releases under the four-eyes principle.
2. **All case data on end devices is encrypted.** AES-256-GCM, with keys held in the operating system key store. A lost device reveals nothing without device lock and app lock.
3. **There is no end-to-end encryption.** Anyone with administrative access to your server process, your database, your file system or your key material can technically read synchronised content. This is a deliberate decision for version 1 and is never presented otherwise.
4. **The software produces your data protection evidence itself.** The record of technical and organisational measures (Art. 32 GDPR), the processor agreement template, the deletion concept and access response letters are generated from the **live configuration of your instance** – not from a boilerplate template. Documentation therefore cannot drift away from reality.
5. **The audit log is protected against the application itself, and keys can be rotated.** The application can neither alter nor delete its own log entries, and every entry is chained to its predecessor — alteration, removal and truncation show up in the check. It does not protect against someone with full database access restoring an older overall state; export the log for that. Encryption keys for device data, attachments and server files can be replaced in live operation.
6. **Two things are missing that you need to know about:** supplied alerting rules for monitoring, and accessibility verified with assistive technology. Both are listed with their status in the section "Open items".

How standards and software relate

This section sounds academic but determines whether your assessment will be sound.

The organisation is certified, not the software

ISO/IEC 27001 certifies a **management system of an organisation** – your organisation. There is no ISO 27001 certification for a software product, and any vendor offering you one is telling you something untrue.

What a piece of software can do is threefold:

1. Implement the **technical measures** of Annex A that your ISMS requires anyway (access control, encryption, logging, protection against malware, and so on).
2. Provide you with the **evidence** you need to demonstrate to your auditor that those measures are effective.
3. **Not stand in the way** of your certification – that is, bring no property that makes a requirement of your ISMS impossible to meet.

Focus Family largely satisfies points 1 and 2. For point 3 you will find a complete, unvarnished list in the section "Where Focus Family currently impedes your certification".

What this means for your assessment

You can file this document as a **supplier disclosure** under your controls A.5.19–A.5.22 (supplier relationships). It replaces neither your own risk assessment nor the data processing agreement – but it provides the factual basis for both.

Division of responsibility: vendor and operator

The most common cause of audit gaps is a control that both parties assumed the other was handling. This table prevents that.

Area	Vendor (Software Notion)	Operator (you)
Encryption on end devices	Implementation, key generation, storage in the OS key store	Enforce device lock, activate app lock by policy
Encryption on the server	File attachments encrypted at rest	**Database and volume encryption**, key custody
Key custody	Generation procedure, documentation	**Backup, separate storage, access protection**
Access control	Role and permission model, server-side enforcement, permission ceiling for account changes, immediate revocation on deactivation	Permission assignment, **periodic recertification of rights**
Two-factor authentication	TOTP and passkeys implemented; sign-in through your own identity provider (OpenID Connect, SAML 2.0)	**Activation by policy** (default: off) or MFA requirement at the identity provider
Logging	Audit log with more than 130 event types, retrieval interface, forwarding of the audit chain to a SIEM (syslog over TLS or CEF)	**Evaluation, retention, alerting, operation of the SIEM**
Backup	Scripts, verified restore procedure	**Execution, retention, encryption, restore tests**
Malware protection	ClamAV integration, fail-closed in production	**Operation and signature updates of the scanner**
Vulnerability remediation	Fixing, provision of new versions as signed updates with downgrade protection	**Applying updates**
Vulnerability reporting	Reporting channel, deadlines and an in-product reporting function	Submit reports; record the deadlines in your supplier file
Retention periods	Configurable; change log, tombstones and access request data are cleaned up automatically	**Set the periods; govern retention of audit and application logs**
Physical security	—	**entirely yours**
Personnel measures	—	**entirely yours** (training, obligations, offboarding)
Interfaces to third-party systems	Standard interfaces, release by the data protection role under the four-eyes principle, privacy presets, disclosure log, transport protection, emergency stop, templates for DPIA and record of processing	**Purpose and legal basis per interface, release, protection and erasure in the target systems, agreements with their operators**
Network access	Restriction of the admin panel to intranet/VPN, fixed proxy network, optional host binding	**Network segmentation, reverse proxy, approval of outbound connections**
Continuity	Offline capability of the apps, restore procedure	**Recovery objectives, continuity exercises, fallback procedures**
Accessibility	Screen reader labels, accessibility statement	Carry the remaining limitations into your own statement

ISO/IEC 27001 – Information security management system

What the software provides

Of the 93 controls in Annex A, 66 can be addressed by software at all; the remaining 27 concern your organisation, your personnel processes and your premises, or are not applicable. Of those 66, **40 are fully implemented and 26 partially, none are open**. Partially means the control is technically present but part of it depends on your configuration or your operations — the details are in the annex.

Particularly well evidenced:

Access control (A.5.15, A.8.2, A.8.3). Every read and write operation is authorised on the server against the current database state – never against assertions made by the client. Visibility filtering happens inside the database query, not afterwards in code. An unauthorised direct request for a known record returns "not found" rather than "forbidden", so it does not even disclose existence.

Segregation of duties (A.5.3). 64 individually assignable permissions, grouped into technical, operational and data protection domains plus two general licence permissions. Administrative rights do **not** extend access to case content. Technical administration and data protection accounts cannot sign in to the apps at all. Data subject access requests are released only under a four-eyes principle. A **permission ceiling** applies to every account change: nobody edits, deactivates or resets the credentials of an account that holds permissions outside their own grant scope; administrators limited to areas only change accounts lying entirely within their areas and never grant organisation-wide administrative rights. Interfaces are set up by technical administration; data flows containing case data are released only by another person holding a data protection permission who neither created nor last changed the interface. Only holders of a dedicated permission review and accept incoming data from interfaces.

Sign-in and revocation (A.5.16, A.5.17, A.5.18, A.8.5). Besides password with TOTP and passkeys, sign-in can be delegated to your own identity provider (OpenID Connect or SAML 2.0, for example Microsoft Entra ID or AD FS); the server continues to issue its own tokens afterwards. Accounts are only linked through identities verified by the provider. With "Enforce SSO" active, local sessions and tokens are revoked when it is switched on; only local system administration accounts keep password access as an emergency route, and only to the admin panel. The strong authentication requirement applies to the panel and to synchronisation under the same rule. A deactivated account loses access at once: sessions and tokens are

revoked and synchronisation rejects stale sign-in states. Sign-in answers uniformly and with equal computing effort for unknown, locked and wrong credentials; account, MFA and emergency access endpoints are rate-limited and lock after failed attempts. Practitioner accounts can be created and deactivated from your own identity management through SCIM 2.0; permissions cannot be changed through SCIM, accounts with administrative permissions are invisible to SCIM, and deactivation revokes the sign-in sessions.

Cryptography (A.8.24). AES-256-GCM for case data on devices and for file attachments on the server, PBKDF2-HMAC-SHA256 with 310,000 iterations for app backups, ECDSA P-256 for device proofs and licence signatures. Credentials, secrets and client certificates of the interfaces are stored encrypted with Data Protection and are never exported; submissions over FIT-Connect are encrypted for the destination, whose key is checked against the public administration PKI. No legacy algorithm is used for any security purpose.

Device binding (A.8.5). Every end device holds its own key pair in the operating system key store. Every request carries a signed device proof; consumed proofs are persisted, so an intercepted proof cannot be replayed. Requests without a device ID are rejected. **Stolen credentials alone are not sufficient for API access.** An app only accepts setup links and QR codes after a two-step confirmation and while unlocked.

End devices (A.8.1). On iOS the app lock appears in a window of its own above all system dialogs. If it cannot be presented, an opaque fallback cover hides the app, and no navigation is possible while the app is locked. On iOS and Android, app data is excluded from cloud and computer backups and from device transfer; if the key is missing after a device change, the app shows a recovery page and never creates a new key over existing data. The navigation trace used for diagnostic reports contains no case identifiers and no parameter values.

Configuration and network (A.8.9, A.8.20, A.8.22). The admin panel can be restricted to the intranet or a VPN; the reverse proxy sits in a fixed network, forwarded client information is trusted only from it, and permitted host names can be set. All administrative actions are protected against request forgery (a regression test checks every action), error pages also carry the security headers, and the licensing service is only contacted over HTTPS outside development. The built-in update procedure refuses downgrades and version mismatches inside the signed package.

Information transfer through interfaces (A.5.14, A.8.21, A.8.26). Standard interfaces are available for connecting line-of-business systems, DMS and electronic records, youth welfare offices, identity management, calendars and SIEM: REST/JSON with OAuth 2.0 client credentials (`private_key_jwt`), webhooks signed according to Standard Webhooks, CMIS 1.1 as client and repository, XÖV/xdomea over directory, SFTP, XTA 2 and FIT-Connect, SCIM 2.0, iCalendar feeds and syslog over TLS or CEF. Every interface carries a purpose and a legal basis and is created as a draft; data flows containing case data become active only after release, and the release is bound to the reviewed state. The presets minimise data: pseudonymised, final documents only, notes and confidential document types blocked, inbound direction off. Every successful transfer relating to a case is recorded in the disclosure log and appears in the subject access package under Art. 15 GDPR. Outbound connections use HTTPS only, follow no redirects, check the target address against SSRF when connecting and can be bound with a custom CA, SPKI pin and mTLS; SFTP requires a confirmed host key. Inbound access requires an IP allow-list (empty means blocked), is rate-limited and bound to areas; delivered files pass type validation and a virus scan, XML is read without DTD processing, packages are only unpacked within size limits. Incoming data lands in an inbox with its own permission. Final erasure of a case also covers the copies held by the interfaces. An emergency stop halts all outbound transfers, repeatedly failing connections pause automatically, and without a valid organisation licence deliveries and access through the interfaces rest; only the forwarding of the audit chain to the SIEM continues.

Data minimisation on devices (A.8.11, A.8.12). Pseudonymised case cover sheets show only placeholders, place of residence and year of birth instead of names, address and date of birth, and contain no phone numbers, e-mail addresses, place of birth, health insurer or child benefit number; Leitweg IDs for e-invoices are stored encrypted; unencrypted temporary and export files only live in folders the app sweeps regularly. Open synchronisation conflicts are encrypted like the rest of the data set, and contact cards and institutions carry no names in the unencrypted search index of the local database.

Protection against malware (A.8.7). Uploaded files pass a type allow-list, magic-byte validation, size limits and a virus scanner. A file is served only after a "clean" verdict. If the scanner is unreachable in production, uploads are **rejected** rather than passed through unscanned.

Change management (A.8.32). Schema changes run exclusively through a transactional migrator with a change ledger and a database lock. A failing step rolls back completely. There is no path for uncontrolled schema drift in operation.

Automatically generated compliance documents (A.5.31, A.5.34). This is the property most valuable to your audit: the record of technical and organisational measures under Art. 32 GDPR, the processor agreement template, the deletion concept and access response letters are generated from the **live configuration of your instance** – including the actually enforced two-factor policy, the configured file types, session duration and account statistics. A divergence between documentation and reality is thereby ruled out.

What you must provide yourself

The software cannot relieve you of 27 of the 93 controls. The most important:

- **Information security policy, risk assessment, statement of applicability, internal audits, management review** – the core of your ISMS.
- **All eight people controls** (A.6): screening, training, confidentiality obligations, arrangements on termination.
- **All fourteen physical controls** (A.7): server room, entry control, storage of mobile devices, secure disposal.
- **Evaluation of logs and alerting.** The software produces the data and offers a retrieval interface; monitoring is your responsibility.
- **Backup and restore testing.** The procedure and scripts are documented and have been executed once with evidence; regular execution is yours.
- **Recertification of access rights.** Assignment is logged; a periodic review must be set up organisationally.
- **Assessment and release of every interface (A.5.14, A.5.19–A.5.22).** Purpose, legal basis, data protection impact assessment and record of processing (templates are supplied), agreements with the operators of the target systems and erasure of the data transferred there are yours.

- **Server clock synchronisation (A.8.17).** The requirement and its verification (`timedatectl status`, `chronyc tracking`) are in the technical handbook; running an NTP service on the host and monitoring it rest with the operator.

Where it currently falls short

Item	Impact on your audit
Two-factor authentication is off by default	A freshly installed instance permits sign-in without a second factor. You must set the policy actively. We recommend making this a mandatory step of your commissioning procedure.
XTA 2 and FIT-Connect only tested against specification mocks	Both transports for file transfer are implemented according to the specification and tested against our own simulations; acceptance against a real counterpart is outstanding (finding F-33). Affects A.8.29. Run a test transfer with your counterpart before productive use.

ISO/IEC 27034 – Application security

What the standard is about

ISO/IEC 27034 describes how a vendor conducts application security **systematically and demonstrably**. Its central idea is that every security control is paired with a **verification measurement** by which its effectiveness can be assessed. Controls are maintained in a library, assigned to a level of trust, and kept current across the application's entire life cycle.

What the software provides

Substantively, a surprising amount is in place – just not under the names the standard uses:

Expectation of the standard	State in Focus Family
Requirements and environment specified	**met** – requirements specification with stable identifiers, acceptance criteria, test evidence, traceability matrix and a concordance that resolves the numbered legacy references in code and documentation
Risks assessed	**met** – 31 threat scenarios with asset, actor, attack, mitigation and **explicitly named residual risk**
Controls paired with verification	**met in substance** – every security control has a test that fails as soon as the control is removed
Application normative framework	**absent**
Targeted level of trust defined	**absent**
Security across the life cycle	**practised, not documented**
Independent assessment	**partial** – several documented assessment rounds including tool-assisted second reviews, all commissioned by the vendor

The pairing of "control and verification" deserves emphasis, because it is what the standard requires at its core and is rarely implemented cleanly: among the 635 test files are deliberate attack tests – access using another tenant's identifiers, privilege escalation through tampered requests, replay of intercepted device proofs, circumvention of the four-eyes release, access across server instances, account changes above one's own permissions, request forgery against every administrative action, timing differences at sign-in, access to internal addresses through interface connections, release of an interface by the person who last changed it, data leaking through the change feed past case visibility. Each of these tests **demonstrates** a security claim rather than merely asserting it.

What you must provide yourself

27034 addresses the vendor primarily. What is relevant for you: you should be able to require the vendor to state the **targeted level of trust** and to set out which controls are verified for it. We can currently give that account descriptively, but not in the structure the standard envisages.

Where it currently falls short

The requirements specification is included (`docs/requirements/REQUIREMENTS.md`). It lists functional, non-functional and security requirements with stable identifiers and test evidence. The original documents behind the paragraph references ("§120", "§175") have not been preserved; a concordance resolves those references from their context. It is a reconstruction, not the original.

There is no control library and no level of trust. The substance exists; the form does not. From the threat model and the existing verification tests, a conformant structure can be derived with moderate effort – this offers the best ratio of effort to benefit of all four standards.

ISO/IEC 25010 – Software product quality

The standard describes product quality through nine characteristics. Assessment in detail:

Functional suitability – met

The operational workflow (prepare → accompany → follow up → document) is fully represented, documented in four manuals and an interfaces manual across two languages, and safeguarded by more than 2,200 server tests and 635 test files overall. The ratio of C# test code to C# production code is 0.63 (133,978 to 213,799 lines) – unusually high for a line-of-business application.

Performance efficiency – partial

The usual provisions are in place: more than 110 database indexes, read queries without change tracking, streaming processing for large files instead of loading them into memory, storage quotas per organisation with atomic reservation, and metrics for disk space and process size through a monitoring interface.

Load evidence: a load test with realistically signed-in devices and signed requests (`docs/server/CAPACITY.md`) stayed error-free with 50 concurrently synchronising virtual practitioners and a pull duration below 250 ms (p95). The resulting sizing statement: up to 200 concurrently working practitioners with the default synchronisation interval are covered with ample headroom on a server with 4 vCPUs and 8 GB RAM. For larger organisations you should repeat the measurement with the supplied script on your target hardware.

What is missing: under overload the server answers with errors instead of letting requests wait, because the connection pool is as large as the database's connection limit (finding F-32).

Compatibility – met

Focus Family runs from a single code base on iOS, iPadOS, Android, macOS and Windows, plus an Apple Watch companion app. Data exchange is deliberately open: case exports as JSON with a supplied schema, time and mileage data as documented CSV, documents as PDF, DOCX and XLSX. The interface is versioned and returns 71 structured error codes.

For connecting your own line-of-business systems, machine-readable interface descriptions in OpenAPI 3.1 format are supplied (`docs/api/openapi.v1.json` for app and administration, `docs/api/openapi.integration-v1.json` for the integration API with its own error codes); automated tests ensure they match the shipped interface. Interoperability with third-party systems relies on open standards rather than proprietary formats: CMIS 1.1 for DMS and electronic records, XÖV/xdomea 3.1.0 and 4.0.0 validated against the official schema, SCIM 2.0, iCalendar, syslog per RFC 5424/5425 and CEF, CloudEvents with Standard Webhooks signatures. Every interface has its own documentation. CMIS and SFTP have been tested against real test systems; XTA 2 and FIT-Connect so far only against simulations of the specification (finding F-33).

Interaction capability – partial

On the positive side: user interfaces of the app, the desktop application and the admin panel in seven languages (German, English, Spanish, French, Turkish, Russian, Polish), consistent tablet and desktop layouts, contextual help and explanatory texts, four manuals tailored to their audiences.

Accessibility, as assessed: every purely symbolic control carries a screen-reader label (60 in the mobile app, 30 in the desktop application), form fields are labelled, the administration interface has a skip link and a visible keyboard focus, text scales with the system setting, and light and dark modes exist. An accessibility statement is enclosed; an automated test fails as soon as a symbolic control without a label is added.

What is missing, and important for you: there has been **no test with real assistive technology** (VoiceOver, TalkBack, NVDA, JAWS), contrast values are unmeasured, reading order and heading hierarchy of the mobile views are unverified, generated PDF documents are untagged, and drawing surfaces (sketches, handwriting, signatures) have no equivalent alternative. Focus Family is therefore **partially conformant** with EN 301 549.

If you are a public-sector body this affects you directly: accessibility regulations oblige you for the information technology you deploy, and the European Accessibility Act broadens those requirements further. Carry the listed limitations into your own accessibility statement; the details are in finding F-13 of the assessment report.

Reliability – met

The most important property for your deployment: **a server outage does not interrupt fieldwork.** The apps work entirely against their local encrypted data store; synchronisation is background reconciliation, not a precondition for working.

Further safeguards: concurrent changes produce a visible conflict rather than a silent overwrite. Repeated transmissions create no duplicates. Deletions leave tombstones, so a long-offline device cannot resurrect deleted data. Restoring an app backup validates the file **completely before** anything is overwritten – a wrong password cannot destroy half a data set. The server's readiness probe genuinely checks the database. Enrolment of a server installation with the licence server is recorded before the installation key is redeemed, and an interrupted attempt can be repeated with the same key; an unreadable licence state produces an error message instead of a silent re-enrolment.

Limitation: the server is designed as a single instance. High availability is yours to arrange.

Security – met

See the ISO/IEC 27001 section. In addition: traceability and non-repudiation are covered by the audit log, document signatures and checksums – subject to the limitation regarding write protection of the log noted in that section.

Maintainability – met

17 clearly delineated sub-projects with clean layering (platform-free domain logic, separated infrastructure, separate user interfaces per platform). Consistent correlation identifiers make a transaction traceable across client, server and log. Test coverage is measured: 87.9 % of lines and 68.0 % of branches. A binding rule set for static security analysis and a scan of the container images run in the build.

Flexibility – met

Five platforms from one code base. Self-hosting with no vendor dependency. Central configuration points for branding and organisational data. Organisation-wide settings can be prescribed centrally and locked on devices.

Safety – partial

Focus Family deliberately makes **no professional decisions**: no diagnoses, no legal assessments, no evaluation of persons. This is stated explicitly in the product description and is upheld in the functionality. Security-relevant mechanisms fail closed in case of doubt (no virus scanner – no upload; missing signing key – rejection).

What is missing: a documented hazard analysis for the operational context. For example: what consequence does the loss of a case journal have for an ongoing support process, and which provision addresses it? Technically the ground is covered (no silent data deletion, conflict surfacing, tombstones), but the reasoning is not written down.

ISO/IEC 29147 and 30111 – Handling vulnerabilities

What they cover

The two standards form a pair. **29147** governs the outward face: how can someone report a security vulnerability to the vendor, and how does the vendor inform operators? **30111** governs the inward process: how does the vendor receive, assess, remediate and publish.

For you as an operator this is not a formality. Your own ISMS requires you to be informed about security updates to the software you deploy, and to be able to assess them.

Current state

Requirement	Standard	State
Published vulnerability disclosure policy	29147	**in place** (`SECURITY.md` in the project, linked from the product page)
Reporting channel (contact address, `security.txt`)	29147	**in place** (`security@software-notion.de`, `/.well-known/security.txt`)
Acknowledgement and response times	29147	**published** (acknowledgement 3 working days, triage 10 working days, remediation 14/30 days by severity)
Coordinated disclosure	29147	**90-day period published, never yet applied**
Security advisories to operators	29147	**template and delivery route defined, no advisory delivered yet**
Receipt and recording of reports	30111	**mailbox in place, reporting function in admin panel, app and desktop**
Verification of reported vulnerabilities	30111	**practised**
Remediation with evidence of effectiveness	30111	**practised**
Release of the remediation	30111	**route defined (signed update with downgrade protection), not yet used for a security fix**
Described process with roles and deadlines	30111	**in place** (`docs/security/VULNERABILITY-HANDLING.md`)
Severity rating (CVSS v3.1)	30111	**defined**

What already works in practice

The substantive part of 30111 is practised and evidenced: several documented assessment rounds, among them a full review in seven parts with 83 individual findings, a tool-assisted second review on 8 October 2026, several review rounds of the integration interfaces from 28 October to 1 November 2026 and, most recently, review rounds of the data room, session renewal and licence lock from 4 to 8 November 2026; each finding was confirmed in the code before remediation, remediated and, where possible, safeguarded by a test that fails if the fix is reverted. The few remaining points left open on purpose are named in the findings report. In addition, every build of the product runs an automatic check of all third-party libraries against known vulnerabilities – a finding **aborts the build**, and does so from severity "low" upwards. That is stricter than common practice. In addition, a static security analysis checks the vendor's own code and a scan checks the container images; both fail on findings without a documented justification.

What this means for you today

Three practical points you should plan for:

1. **You can report right away.** The channel is `security@software-notion.de`, published in `security.txt` and in the disclosure policy; the admin panel, the app and the desktop application contain a reporting function that compiles technical details without case or personal data. Record the address in your supplier file.
2. **Security advisories for releases are prepared but have never been sent.** Template and delivery route are defined; since no release has yet had to close a reported vulnerability, there is no example to show. Agree with us which address in your organisation such advisories should reach.

3. **Response times are published, not contractual.** Acknowledgement within three working days, triage within ten working days, remediation within 14 days for critical and 30 days for high severity. If your ISMS requires supplier deadlines, take these values into the contract.

The outward side under 29147 is therefore in place; what is missing is evidence from operation, because no incident has yet run through the process. That is the reason for the rating "in place, not yet exercised".

Where Focus Family currently impedes your certification

This is the list you as an assessor are actually after. It contains everything an auditor could turn into a non-conformity or a condition at your organisation.

#	Item	Affected control	Action required of you
1	Advisories for releases prepared, not yet delivered	29147	Agree the delivery route with us
2	Accessibility partially implemented, not tested with assistive technology	25010, EN 301 549, BITV 2.0	The accessibility statement is enclosed; carry the remaining limitations into your own statement
3	Two-factor authentication disabled by default	27001 A.8.5	Set actively at commissioning – mandatory step
4	No end-to-end encryption on the server side	27001 A.8.24, GDPR Art. 32	Govern and document operator access organisationally
5	No remote wipe for lost devices	27001 A.8.1	Provide your own device lock or mobile device management
6	Capacity evidenced up to 200 concurrently active practitioners; overload yields errors instead of waiting	25010 performance efficiency	Plan your own load test on the target hardware beyond that
7	No alerting rules supplied	27001 A.8.16	Define your own thresholds (the data sources exist)
8	Server designed as a single instance	25010 reliability	Define your own recovery objectives
9	No independent external security assessment	27001 A.5.35	Consider commissioning your own penetration test
10	Server information retrievable without sign-in	27001 A.8.9	Do not expose the server publicly without need, restrict the admin panel to the intranet or VPN
11	Screenshots only technically prevented on Android; on iOS only the app-switcher preview is hidden, the desktop app offers no screen protection	27001 A.8.12, A.8.1	Block screenshots on managed iOS devices via MDM, include the rule in the staff instructions
12	File transfer over XTA 2 and FIT-Connect only tested against specification mocks	25010 compatibility, 27001 A.8.29	Run a test transfer with your own counterpart before productive use

---

Deliberate limits of the product

These properties are decisions, not oversights. You should be aware of them and reflect them in your risk assessment.

No end-to-end encryption. Anyone with administrative access to the server process, the database, the file system or the key material can read synchronised content. Marking an entry as "private" protects it from **other users of the application** – including team leads and every administrative role – but not from the operator of your infrastructure. The software never presents this differently.

No remote wipe. Revoking a device's access takes effect on the server immediately, but on a permanently offline device only at its next connection. Until then, local encryption, the app lock and the limited validity of the offline grant provide protection. We explicitly promise **no** immediate remote wipe.

Server content is not encrypted at application level. Protection of data at rest on the server is provided by encryption of your storage volume – with the exception of file attachments, which are additionally encrypted at the application layer. Encrypting the database volume is your responsibility.

No requirement to be online. This is a strength, but it has a flip side: data on a device that never synchronises exists only there. Because app data enters neither cloud nor computer backups nor a device transfer, a new device starts with setup; data returns through an app backup or synchronisation. Your specifications for synchronisation frequency and app backups are therefore also a data protection measure in the sense of availability.

No erasure in target systems. Whatever an interface has transferred to a DMS, an electronic record system, a youth welfare office or another third-party system is not erased there by Focus Family. Final erasure of a case removes the copies inside Focus Family; for the target systems the delivery log names the recipients, and on request a webhook event without content reports the requested erasure. Retention and erasure in the target systems are your responsibility.

No analytics, tracking or advertising components. There is no telemetry to the vendor. Crash reports go exclusively to **your** server, contain technical fields only and are redacted on the device itself – no case data, no names, no content. Sending is on by default and can be switched off in the settings of every application.

Data protection and openness

A section of its own, because both are explicit product goals.

No vendor lock-in for your data

- **Self-hosting.** The server runs in your infrastructure. There is no vendor cloud that case data flows to, and no route by which we could access your content.
- **Open export formats.** Case exports as JSON with a **supplied schema**; time and mileage data as CSV with documented column semantics; documents as PDF, DOCX and XLSX. You can extract your entire data set at any time and continue using it in another system.
- **Documented synchronisation protocol.** Some 470 lines of protocol description, plus a dedicated contracts module with 71 named error codes and an interface description in OpenAPI 3.1 format.
- **Standard interfaces.** REST/JSON with an OpenAPI description, CMIS 1.1, XÖV/xdomea, SCIM 2.0, iCalendar and syslog/CEF, each with its own documentation and a configuration export without secrets.
- **Documented database schema and migration path.** A database dump can be interpreted without our involvement.

Data protection as a product feature

The full procedure for data subject rights under Art. 15–21 GDPR is implemented in the product, not merely described: search, identity verification, collection, screening for mentions of third parties under Art. 15(4), redaction, release under a four-eyes principle, encrypted handover with a single-use download, automatic deletion after the retention period, and a complete log of every access. One request can cover several data subjects, which matches the family-oriented structure of your cases. If processing of a record is restricted under Art. 18, the server also blocks download and existence checks of its attachments through the device interface; the response is the same as for an unknown file. The access package lists, from the disclosure log, the recipients to which interfaces have transferred data of the data subjects, with purpose and legal basis at the time of transfer.

Where openness currently ends

For the sake of honesty: the source code is **not** disclosed. A machine-readable software bill of materials in CycloneDX format is generated during the build and supplied on request; the overview of third-party libraries is checked automatically against the versions actually used.

Open items and planned improvements

For completeness, with an honest indication of effort. No commitment to dates is implied; please ask us for the current status.

Intended measure	Effect	Effort
Two-factor authentication on by default	Secure default configuration	low
Connection pool with back-pressure, less log volume in production	Waiting instead of errors under overload	low
Reduced server information before sign-in	Hinders reconnaissance	low
Acceptance of XTA 2 and FIT-Connect against real counterparts	Evidences file transfer within public administration	medium
Supply alerting rules, forward application logs	Monitoring without writing your own rules	medium
Derive a control library and level of trust	Makes 27034 arguable	medium
Test accessibility with assistive technology, measure contrast, tag PDFs	Closes the remaining accessibility gap	high
Independent penetration test	External confirmation	high

Evidence register

For every statement in this document, the artefact that substantiates it. All listed materials are supplied with the product or made available on request.

Statement	Evidence
Encryption methods and key management	Security documentation, sections on the encryption model and key management
Threats and residual risks	Server threat model, 28 scenarios, seven of them on the interfaces
Access and permission model	Permissions documentation and authorisation documentation
Synchronisation and conflict handling	Synchronisation protocol documentation
Effectiveness of security controls	Automated test suite, 635 test files including deliberate attack tests
Test coverage, static analysis, image scanning	Overview of quality and security checks (`docs/security/QUALITY-GATES.md`) with reports per run
Load and capacity	Measurement report with sizing statement (`docs/server/CAPACITY.md`)
Interface description	`docs/api/openapi.v1.json` and `docs/api/openapi.integration-v1.json` (OpenAPI 3.1)
Interfaces to third-party systems	Documentation per interface (`docs/integration/`), interfaces manual, data protection and security of the interfaces with templates for DPIA and record of processing plus a hardening checklist (`docs/integration/SECURITY-PRIVACY.md`), decision D16
Internal security assessments	Audit reports with individual evidence per finding, full review of 3 October 2026; tool-assisted second review of 8 October 2026 and reviews of the desktop update, Paddle billing and deletion jobs from 22 to 24 October 2026, review rounds of the integration interfaces from 28 October to 1 November 2026 and review rounds of the data room, session renewal and licence lock from 4 to 8 November 2026, each with fixes and regression tests in the changelog
Sign-in through the identity provider	Technical handbook, chapter on single sign-on; permission documentation
Technical and organisational measures (Art. 32)	Generated in the admin panel from your live configuration
Data processing agreement	Processor agreement template, generated in the admin panel
Deletion concept	Generated in the admin panel from your configuration
Data subject rights	Documentation of the access request procedure
Backup and restore	Procedure documentation with a completed restore test
Vulnerability disclosure and handling	Disclosure policy (`SECURITY.md`), `/.well-known/security.txt` , handling process (`docs/security/VULNERABILITY-HANDLING.md`), advisory template
Accessibility	Accessibility statement (`docs/ACCESSIBILITY.md`), automated test for missing labels (`AccessibilityLabelTests`)
Incident procedures	Six runbooks for the most likely incidents
Commissioning and operation	Technical manual and deployment runbook
Third-party libraries and licences	Third-party component overview (checked automatically against the versions used), CycloneDX bill of materials
Requirements and traceability	Requirements specification (`docs/requirements/REQUIREMENTS.md`) with traceability matrix and concordance of legacy references
Time synchronisation	Technical handbook, requirements and section "Checking time synchronisation"; requirement NFR-OPS-01
This assessment in detail	Companion document "Findings and Remediation Plan"

Questions you should be asking us

If you are conducting this assessment seriously, these are the points to press on. We have written them down ourselves deliberately.

1. How do you evidence the write protection of the audit log?
2. Through which channel and within what deadline do we report a security vulnerability to you?
3. How will we learn that a new version closes a security vulnerability?
4. What response times do you commit to by severity, and are they in the contract?
5. Can you supply a machine-readable bill of materials for all third-party libraries?
6. What is the status on accessibility, and is there a credible plan?
7. Does an independent security assessment exist, and may we see the report?
8. How are requirements linked to implementation and tests, and how do you resolve the paragraph references in code and documentation?
9. For what order of magnitude has the system been tested with evidence?
10. How do you ensure that the statements in this document remain current?
11. How does administration remain reachable if our identity provider fails, and who may still access it then?
12. Which data leaves our installation through interfaces, who releases it, and how do data subjects learn about it?

Contact and validity

This document describes product state 1.4.0 (build 26308), assessed on 8 November 2026. It loses its validity with every material change to the product. Please request a current version before making a procurement decision.

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

A German version of this document is available on request.