TAIGA

DATA PROTECTION IMPACT ASSESSMENT

Data Protection Impact Assessment

ORGANIZATION defence

DATE April 14, 2026

Table of Contents

Necessity and Proportionality Assessment

Business Necessity

The processing of personal data in Hälytin is strictly necessary for the stated purpose of delivering air-threat alerts to Finnish residents. The necessity assessment examines whether the system could achieve its goal with less data or through less intrusive means.

Purpose and Necessity Justification

Primary Purpose: Deliver real-time air-threat alerts from FDF air surveillance to affected civilians within seconds of threat detection.

Why this processing is necessary:

1. **Device Token Collection**
    - **Necessity**: Required to route push notifications to the correct device
    - **Why it cannot be avoided**: Push notification infrastructure (APNs, FCM) requires a unique device identifier to deliver messages
    - **Minimization**: Tokens are stored as one-way hashes server-side; raw tokens are never persisted in plaintext; tokens are not used for any purpose other than alert delivery
    - **Proportionality**: The burden on data subjects (permission grant during onboarding) is minimal; the benefit (life-saving alert) is substantial
2. **Coarse Location (Municipality-Level)**
    - **Necessity**: Required to target alerts to the geographic area affected by the threat
    - **Why it cannot be avoided**: Nationwide alerts for localized threats erode public trust and violate the design principle of geographic precision (municipality granularity minimum per spec)
    - **Alternatives considered and rejected**:
        - **Precise GPS location**: Rejected because (a) it exceeds the minimum necessary for alert targeting, (b) it creates a persistent location-tracking dataset, (c) it increases privacy harm and regulatory risk, (d) municipality-level precision is sufficient for alert targeting
        - **No location data**: Rejected because it would require nationwide alerts for all threats, reducing effectiveness and eroding trust
        - **Cell broadcast only (Phase 2)**: Deferred to Phase 2 because it requires carrier and regulatory work; Phase 1 relies on app-based targeting
    - **Minimization**: Location is coarse (municipality-level); no precise GPS is retained server-side; location is derived from device registration or cellular location, not from continuous GPS tracking
    - **Proportionality**: The burden (location permission during onboarding) is modest; the benefit (targeted alerts that apply to the user) is substantial
3. **Language Preference**

- **Necessity**: Required to render alert content in the user's preferred language (Finnish, Swedish, or English)
- **Why it cannot be avoided**: Alerts must be comprehensible to users; language preference is the minimum data needed to select the correct language variant
- **Minimization**: Language preference is a single enumerated value; no linguistic content analysis or profiling
- **Proportionality**: Minimal burden; substantial benefit (alert comprehension)

4. **Accessibility Flags**
   - **Necessity**: Required to deliver alerts in accessible formats (high contrast, large type, vibration-only for deaf users)
   - **Why it cannot be avoided**: WCAG 2.2 AA conformance requires the system to adapt alert rendering to accessibility needs
   - **Minimization**: Flags are boolean or enumerated values; no continuous monitoring or profiling
   - **Proportionality**: Minimal burden; substantial benefit (accessibility compliance and user safety)

5. **Install Timestamp**
   - **Necessity**: Required for aggregate reach metrics (e.g., "X installs in the first 24 hours") used to assess public awareness campaign effectiveness
   - **Why it cannot be avoided**: Reach metrics are essential for program accountability to Sisäministeriö and parliamentary oversight
   - **Minimization**: Timestamp is aggregated only; no per-user temporal tracking or profiling
   - **Proportionality**: Minimal burden; substantial benefit (program accountability)

6. **Operator Identity and Actions**
   - **Necessity**: Required for accountability and post-incident review; enables investigation of false alerts or missed alerts
   - **Why it cannot be avoided**: An emergency response system without audit trails is unaccountable and untrustworthy
   - **Minimization**: Operator identities are managed by external identity provider (Virtu/Suomi.fi); no raw passwords stored
   - **Proportionality**: Operators are government employees subject to security clearance; the burden is consistent with their role

7. **Audit Log Entries**
   - **Necessity**: Required for legal accountability, regulatory compliance, and post-incident review
   - **Why it cannot be avoided**: Finnish recordkeeping rules and government accountability standards require auditable records of emergency response actions
   - **Minimization**: Audit entries are structured and limited to state-changing operations; no continuous event logging
   - **Proportionality**: Substantial benefit (accountability and oversight); minimal burden (passive logging)

Data Minimization: Alternatives Considered and Rejected

Alternative	Why Rejected	Residual Risk
Nationwide alerts for all threats	Violates geographic precision principle; erodes public trust; reduces effectiveness; citizens learn to ignore alerts that don't apply to them	High: system becomes useless if users stop trusting alerts
Precise GPS location instead of municipality	Exceeds minimum necessary; creates persistent location-tracking dataset; increases privacy harm; municipality-level is sufficient for alert targeting	Medium: location privacy violation; regulatory risk
No location data; use device IP address	IP address is less reliable than municipality code; requires continuous IP logging; exceeds minimum necessary	Medium: location privacy violation; IP tracking risk
User account registration for alert preference	Increases friction during onboarding; reduces install rate; violates privacy-by-design principle (anonymous by default); no additional benefit over current model	High: reduced install base = reduced alert reach
Continuous device health monitoring	Exceeds minimum necessary; creates behavioral tracking dataset; no benefit to alert delivery	High: privacy violation; regulatory risk
Integration with national identity register (PREH)	Exceeds minimum necessary; links alerts to personal identity; violates anonymity principle; no benefit to alert delivery	Critical: transforms system from anonymous to identified; major privacy violation
Retention of device tokens after uninstall	Exceeds minimum necessary; enables device fingerprinting; violates data minimization principle	High: privacy violation; enables surveillance

Proportionality Assessment

Balancing Test (comparing benefits to privacy harms):

Factor	Assessment	Weight
Necessity of processing	Essential for vital-interest purpose (life safety); no less intrusive alternative exists	Critical
Scale of processing	Large-scale (5.5M potential data subjects, 3M+ active users); but data is pseudonymized and minimized	High
Nature of personal data	Coarse location, device identifier (hashed), language preference; not sensitive categories (health, biometric, genetic)	Medium
Vulnerability of data subjects	General population including children and elderly; but alert delivery is protective, not exploitative	Medium
Expectations of data subjects	Users voluntarily install app and grant permissions; explicit privacy notice provided; users can uninstall at any time	Low (supports proportionality)
Sensitivity of data	Device tokens and location are moderately sensitive; but municipality-level location is coarse; tokens are hashed	Medium
Retention period		

Short-term for device data (until uninstall); long-term for audit logs (10 years); justified by legal obligation	Medium	
Security measures	Encryption at rest and in transit; RBAC; audit logging; secrets management; vendor security assessments	Low (supports proportionality)
Availability of data subject rights	Full GDPR rights supported (access, erasure, portability, restriction, object); implemented at application layer	Low (supports proportionality)
Legitimate interests of the controller	Public task (emergency response); vital interests (life safety); no commercial interest	Critical (supports proportionality)

Conclusion: The processing is proportionate. The benefits (rapid life-saving alerts to millions of residents) substantially outweigh the privacy harms (pseudonymized device data, coarse location, minimal retention). The privacy-by-design approach (anonymous by default, minimized data, user control) further reduces the proportionality concern.

Necessity Relative to Legal Basis

Vital Interests (GDPR Article 6(1)(d)):

- Processing is necessary to protect the life and physical safety of data subjects
- In an air-threat scenario, rapid notification is essential
- Data subject cannot consent in real-time
- Vital interests override other legal bases
- Proportionality: Processing is proportionate to the vital interest (life safety)

Public Task (GDPR Article 6(1)(e)):

- Processing is necessary for the performance of emergency response (public task)
- Operator and audit data are necessary for accountability
- Processing is authorized by law (Act on Emergency Response Centre Operations, Rescue Act, Cybersecurity Act)
- Proportionality: Processing is proportionate to the public task (emergency response accountability)

Least Intrusive Alternative Assessment

For each data element, the least intrusive alternative was selected:

Data Element	Alternative Considered	Selected Approach	Why Selected
Device token	Store raw token	Store hashed token only	Hashing is one-way; prevents device fingerprinting; sufficient for spam prevention
Location	Precise GPS	Municipality code	Coarse location is sufficient for alert targeting; reduces privacy harm
Language	Infer from device locale	User selection	User selection is more accurate; respects user autonomy

Accessibility	Infer from device settings	User selection	User selection is more reliable; respects user autonomy
Install timestamp	Continuous telemetry	Single registration timestamp	Single timestamp is sufficient for reach metrics; reduces surveillance risk
Operator identity	Anonymous logging	Named operator logging	Accountability requires identity; security clearance mitigates abuse risk
Audit entries	Sampling (1% of events)	All state-changing events	Complete audit is necessary for accountability; sampling would hide failures

Conclusion on Necessity and Proportionality

The processing of personal data in Hälytin is strictly necessary for the stated vital-interest purpose (life-saving alert delivery) and the public-task purpose (emergency response accountability). The data collected has been minimized to the absolute minimum required; less intrusive alternatives have been considered and rejected as insufficient. The proportionality assessment confirms that the benefits (rapid life-saving alerts to millions of residents) substantially outweigh the privacy harms (pseudonymized, minimized data with strong security controls). The privacy-by-design approach (anonymous by default, user control, no commercial use) further supports proportionality.

The necessity and proportionality assessments align with GDPR Article 5(1)(c) (data minimization) and Article 25 (privacy by design and by default).

Consultation and Stakeholder Engagement

This section documents the consultation process required by GDPR Article 35(9) and identifies stakeholders whose views should be obtained on the DPIA.

Mandatory Consultation

Data Protection Officer (DPO)

Requirement	Status	Details
DPO involvement in DPIA process	Required	Hätäkeskuslaitos has not designated a DPO (not required by GDPR Art. 37 because Hätäkeskuslaitos is not a public authority in the Art. 37(1)(a) sense, nor does it perform large-scale systematic monitoring). However, best practice is to engage a privacy officer or external DPO for this assessment.
DPO review and advisory opinion	Required	External DPO or privacy officer should review this DPIA and provide written advisory opinion before system launch.
DPO sign-off	Required	DPO approval required before system enters production.

Supervisory Authority Consultation (GDPR Article 36)

Condition	Applicable	Action
Residual risk remains high after mitigation	No	Residual risks are Low to Medium after mitigation; no risks remain Critical or High. Prior consultation with supervisory authority is not required.
Processing likely to result in high risk	No	Processing is privacy-minimized (anonymous device data, coarse location, no profiling); mitigations are strong; high risk is unlikely.
Supervisory authority has issued guidance	Yes	Tietosuojavaltuutettu (Finnish Data Protection Ombudsman) has issued guidance on emergency alert systems; this DPIA aligns with that guidance.

Conclusion on Supervisory Authority Consultation: Prior consultation with the supervisory authority is not required under Article 36(3). However, Hälytin should maintain communication with Tietosuojavaltuutettu throughout the project lifecycle and notify them of the system before launch (Article 36(5) — notification of high-risk processing).

Recommended Consultation

Internal Stakeholders

Stakeholder	Role	Consultation Purpose	Recommended Engagement
Hätäkeskuslaitos Legal & Compliance	Legal review	Verify DPIA aligns with legal obligations under Rescue Act, Emergency Re-	Review and sign-off before launch; quarterly review during operation

		sponse Centre Act, Cybersecurity Act	
Hätäkeskuslaitos Information Security	Security assessment	Verify mitigations are technically feasible and aligned with security architecture	Review and sign-off before launch; quarterly security audit
Hätäkeskuslaitos Operations	Operational feasibility	Verify consent/rights processes are operationally sustainable; operator training requirements	Review before launch; input into operator training plan
Sisäministeriö Preparedness Division	Program stakeholder	Verify DPIA aligns with program objectives; input on acceptable risk levels	Review and approval before launch; annual review
Sisäministeriö Legal & Compliance	Legal review	Verify DPIA aligns with government data handling standards	Review and sign-off before launch
Taiga AI Security Team	Vendor security	Verify Taiga's security controls are adequate; confirm compliance with contract obligations	Review and sign-off before launch; quarterly security updates

External Stakeholders

Stakeholder	Interest	Consultation Purpose	Recommended Engagement
Tietosuojavaltuutettu (Data Protection Ombudsman)	Privacy oversight	Provide feedback on DPIA; flag any concerns about processing	Notify before launch; respond to any inquiries; annual reporting
Traficom NCSC-FI (Cybersecurity Centre)	Security assessment	Verify PiTuKri compliance; review security architecture	Engage during PiTuKri assessment process (Phase 1 MVP)
Suojelupoliisi (Finnish Security Police)	Facility security clearance	Verify Facility Security Clearance requirements; review physical security measures	Engage during FSC application process (critical path)
Puolustusvoimat — Pääesikunta (Defence Command)	FDF data handling	Verify classified data handling complies with military security standards; review FDF intake interface	Engage during threat object schema specification; quarterly security review
Apple and Google	Data processor	Verify data handling practices; review privacy commitments; confirm SCCs are in place	Engage during integration phase; annual data processor agreement review
Mobile carriers (DNA, Elisa, Telia)	Data processor	Verify SMS gateway data handling; confirm no unnecessary data retention	Engage during SMS integration; annual data processor agreement review
Citizens and civil society	Data subject interests	Gather feedback on privacy concerns; test comprehensibility of privacy notice	User testing during app development; feedback form during operation

Consultation Process and Timeline

Phase 1: Internal Review (April-May 2026)

1. **Week 1-2**: DPIA completed; shared with Hätäkeskuslaitos Legal & Compliance and Information Security for internal review

2. **Week 3**: Internal review feedback incorporated; DPIA revised
3. **Week 4**: DPIA shared with Sisäministeriö Preparedness Division and Legal & Compliance for program-level review
4. **Week 5**: Program-level feedback incorporated; DPIA finalized

Phase 2: External Review (May-June 2026)

1. **Week 1**: DPIA shared with external DPO for advisory opinion (2-week review window)
2. **Week 3**: DPO feedback incorporated; DPIA revised
3. **Week 4**: DPIA shared with Traficom NCSC-FI and Suojelupoliisi as part of compliance assessment process
4. **Week 5-8**: Compliance assessment feedback incorporated; DPIA finalized

Phase 3: Pre-Launch Notification (June 2026)

1. DPIA finalized and approved by DPO, Hätäkeskuslaitos, and Sisäministeriö
2. Notification sent to Tietosuojavaltuutettu (Data Protection Ombudsman) per Article 36(5)
3. DPIA published on halytin.fi (summary version for public transparency)
4. System clears go-live gate for privacy compliance

Phase 4: Ongoing Consultation (Post-Launch)

1. **Quarterly**: Security and privacy updates shared with Hätäkeskuslaitos and Sisäministeriö
2. **Annual**: DPIA reviewed and updated; consultation with DPO and supervisory authority
3. **As-needed**: Response to any inquiries from Tietosuojavaltuutettu or other stakeholders

Consultation Questions and Expected Input

For DPO / Privacy Officer:

- Is the DPIA compliant with GDPR Article 35 requirements?
- Are the privacy risks adequately identified and assessed?
- Are the mitigations proportionate and effective?
- Are data subject rights adequately supported?
- Should any additional safeguards be implemented?
- Are there any concerns about the lawful basis (vital interests vs. public task)?
- Should the supervisory authority be consulted?

For Hätäkeskuslaitos Legal & Compliance:

- Does the DPIA align with legal obligations under Rescue Act, Emergency Response Centre Act, Cybersecurity Act?
- Are retention periods compliant with Finnish recordkeeping rules?
- Are there any legal gaps or conflicts?
- Should any additional legal safeguards be implemented?

For Hätäkeskuslaitos Information Security:

- Are the security mitigations technically feasible?
- Are there any security gaps or conflicts with security architecture?
- Should any additional security controls be implemented?
- Are the mitigations aligned with SEC policy requirements?

For Sisäministeriö Preparedness Division:

- Does the DPIA align with program objectives?
- Are the acceptable risk levels appropriate for an emergency response system?
- Should any additional safeguards be implemented?
- Are there any operational concerns?

For Traficom NCSC-FI:

- Does the DPIA align with PiTuKri compliance requirements?
- Are the security controls adequate for TL III data processing?
- Should any additional security measures be implemented?

For Suojelupoliisi:

- Are the facility security measures adequate for classified data handling?
- Should any additional physical security measures be implemented?
- Are there any concerns about the FDF intake interface?

For Citizens and Civil Society:

- Is the privacy notice clear and comprehensible?
- Are there privacy concerns not addressed in the DPIA?
- Are the data minimization measures adequate?
- Are data subject rights adequately supported?

Consultation Documentation

All consultation activities will be documented and retained:

Documentation	Retention	Owner
Consultation request emails	2 years	DPO
Stakeholder feedback and comments	2 years	DPO
DPIA revision history	5 years	DPO
Approval signatures and sign-offs	10 years	DPO
Consultation meeting notes	2 years	DPO
Supervisory authority communications	5 years	DPO

Escalation Path

If consultation reveals material concerns or objections:

1. **Concern raised**: Stakeholder submits concern in writing with specific rationale
2. **Initial response**: DPO or data controller responds within 5 business days
3. **Escalation (if concern not resolved)**: Concern escalated to Hätäkeskuslaitos Director General or Sisäministeriö Preparedness Division Director
4. **Resolution**: Concern addressed through DPIA revision, additional safeguards, or risk acceptance decision
5. **Documentation**: All escalations and resolutions documented in DPIA record

Ongoing Stakeholder Engagement

Post-launch stakeholder engagement will include:

- **Quarterly security briefings** to Hätäkeskuslaitos and Sisäministeriö on privacy and security incidents
- **Annual DPIA review** with DPO and supervisory authority
- **User feedback collection** via in-app feedback form and periodic surveys
- **Incident notification** to Tietosuojavaltuutettu within 72 hours of any data breach (GDPR Article 33)
- **Annual transparency report** to Sisäministeriö and Hätäkeskuslaitos on data subject rights requests, incidents, and compliance

Privacy Risks Assessment

This section identifies risks to data subject rights and freedoms arising from Hälytin's processing activities. Risks are assessed using the likelihood (1-5) and impact (1-5) scale defined in RSK-2, with score = likelihood x impact. Confidence ratings reflect the reliability of the assessment based on input document detail.

Risk Assessment Methodology

Likelihood Scale:

- 5 (Almost Certain): >90% probability in 12 months; attack is trivial; no controls exist
- 4 (Likely): 50-90% probability; attack requires low skill; weak controls
- 3 (Possible): 25-50% probability; attack requires moderate skill/access
- 2 (Unlikely): 5-25% probability; attack requires high skill and specific conditions
- 1 (Rare): <5% probability; attack requires nation-state resources or extreme luck

Impact Scale:

- 5 (Catastrophic): Business failure; regulatory shutdown; safety incident; >1M users affected
- 4 (Major): Significant financial loss (>$1M); regulatory investigation; major reputation damage; 100K-1M users affected
- 3 (Moderate): Material financial loss ($100K-$1M); operational disruption; limited data exposure; 1K-100K users affected
- 2 (Minor): Limited financial loss ($10K-$100K); brief disruption; minimal data exposure; <1K users affected
- 1 (Negligible): Minimal financial loss (<$10K); no data exposure; easily recovered

Confidence Scale:

- High: Risk source explicitly described in input documents; well-defined system behavior; explicit data flows
- Medium: Risk inferred from system type; reasonable assumptions based on architecture; partial documentation
- Low: Significant gaps in documentation; assumptions based on common patterns; extrapolated from limited context

Privacy Risks

Risk ID	Description	Likelihood	Impact	Score	Confidence	Source	Rationale
PR-001	Unauthorized access to device tokens via SQL injection or API abuse	3 (Possible)	4 (Major)	12	High	Data Flow TB-7 (Core API to Database); Spec section 5.1 (API design); Architecture section on API security	Device tokens are hashed server-side, reducing but not eliminating risk. API endpoints are protected by input validation (SEC-6.1), but injection

							attacks remain possible. Impact is Major because token compromise could enable device fingerprinting or location tracking of up to 3M+ users. Likelihood is Possible because (a) injection attacks are common, (b) API is internet-exposed behind WAF, (c) controls exist but may have gaps.
PR-002	Unauthorized access to coarse location data via database compromise	2 (Unlikely)	4 (Major)	8	High	Data Flow section dataInventory; Architecture section on data protection	Location data is encrypted at rest (AES-256, SEC-3.1) and accessed only by Core API (least-privilege access, SEC-2.1). Database is not internet-exposed. Likelihood is Unlikely because (a) encryption is strong, (b) database access is restricted, (c) network segmentation (SEC-4.3). Impact is Major because coarse location of 3M+ users could enable population tracking by municipality.
PR-003							

Device tokens transmitted in plaintext to APNs/FCM due to TLS misconfigu-ration	1 (Rare)	4 (Major)	4	High	Data Flow TB-5 (Core Platform to Push Infrastruc-ture); Architecture section on network security; Spec section 5.2 (integrations)	Tokens are encrypted in transit via TLS 1.3 (SEC-3.2). Misconfigu-ration is rare because (a) TLS is enforced at platform level, (b) certificate pinning is used for APNs (DEF-SEC-2.2), (c) WAF validates outbound TLS (SEC-4.2). Likelihood is Rare. Impact is Major because token compromise could enable device-level attacks.	
PR-004	Location privacy violation via continuous GPS tracking if developer implements unautho-rized location collection	2 (Unlikely)	3 (Moderate)	6	Medium	Spec section 4.3 (sensitive data); Architecture section on data minimization	Specifica-tion explicitly prohibits precise GPS retention server-side (Data Flow dataInvento-ry). Risk is that developer implements unautho-rized location collection despite spec constraints. Likelihood is Unlikely because (a) specification is explicit, (b) code review is part of SDLC, (c) security scanning detects location API calls (SDLC-3.1). Impact is Moderate because location of 1M-3M

							users could enable population tracking. Confidence is Medium because implementation details are not fully specified.
PR-005	Data subject rights requests denied or delayed due to process failure	3 (Possible)	3 (Moderate)	9	Medium	DPIA section dataSubjectRights; Spec section 6.1 (compliance requirements)	Data subject rights are implemented via app features (export, delete, opt-out) and API endpoints (audit log access). Risk is that requests are not processed within 30-day GDPR timeline due to manual review bottleneck. Likelihood is Possible because (a) some requests require DPO review, (b) audit log exports may be large, (c) process is partially manual. Impact is Moderate because GDPR Article 12 violation could result in supervisory authority investigation. Confidence is Medium because process details are not fully specified.
PR-006	Cross-border transfer to APNs/FCM	2 (Unlikely)	4 (Major)	8	High	Data Flow TB-5; Architecture section on	Device tokens are transferred to Apple

	without adequate safeguards					data protection; Spec section 5.2	APNs (USA) and Google FCM (USA) for push notification delivery. Risk is that transfer is not adequately safeguarded under GDPR Chapter V. Mitigations: (a) tokens are hashed server-side (pseudonymized), (b) no precise location transferred, (c) Apple and Google have committed to data protection frameworks (SCCs or EU-US Data Privacy Framework), (d) Transfer Impact Assessment completed. Likelihood is Unlikely because safeguards are in place. Impact is Major because token compromise of 3M+ users could violate GDPR Chapter V.
PR-007	Device data retained beyond necessary retention period due to back-up/archival failure	2 (Unlikely)	3 (Moderate)	6	Medium	Spec section 6.3 (audit and retention); Architecture section on backup and recovery	Device data should be deleted upon uninstall. Risk is that deletion is not cascaded to all data stores (primary database, cache, backups, archives). Likelihood is

							Unlikely because (a) deletion is automated (background job), (b) backups are encrypted, (c) retention policies are enforced by database. Impact is Moderate because retained device data could enable device fingerprint-ing or location tracking. Confidence is Medium because back-up/archival procedures are not fully detailed.
PR-008	Operator identity and audit log data accessible to unautho-rized persons due to RBAC bypass	2 (Unlikely)	4 (Major)	8	High	Data Flow TB-3 (Operator Console boundary); Architecture section on authoriza-tion controls; Spec section 5.2 (authentica-tion & access)	Audit logs and operator identities are sensitive (KÄYTTÖ RAJOITET-TU equivalent). Risk is that RBAC is bypassed via privilege escalation or code injection. Mitigations: (a) RBAC enforced at application layer (SEC-2.6), (b) separate database roles for read/write (least-privi-lege), (c) code review and security scanning (SDLC-3.1), (d) audit logging of all access (ARC-6.5). Likelihood is Unlikely because (a)

							controls are multi-layered, (b) access is restricted to internal network, (c) smart card authentication (SEC-1.3). Impact is Major because audit log compromise could expose operator identities and actions to hostile actors.
PR-009	Privacy notice inadequate or not provided due to process failure	3 (Possible)	2 (Minor)	6	Medium	DPIA section processingOverview; Spec section 6.1 (compliance); Architecture section on API design	Privacy notice is provided during app onboarding before data collection (GDPR Article 13). Risk is that notice is not displayed, is displayed in wrong language, or is incomprehensible. Likelihood is Possible because (a) onboarding flow is complex, (b) localization may have gaps, (c) process is partially manual. Impact is Minor because notice failure is a procedural violation (not data subject harm). Confidence is Medium because onboarding UX details are not specified.

PR-010	Facility security breach at Hätäkeskuslaitos or cloud provider enabling unauthorized access to classified data	1 (Rare)	5 (Catastrophic)	5	High	Data Flow TB-1 (FDF intake boundary); Spec section 6.2 (compliance — Katakri); Architecture section on infrastructure	Pre-dispatch threat data is classified TL III (LUOTTAMUKSELLINEN). Risk is that physical security breach at Hätäkeskuslaitos or cloud provider enables unauthorized access. Mitigations: (a) facility security per KATAKRI F-series (DEF-SEC-3.1 through DEF-SEC-3.6), (b) network segmentation isolates FDF DMZ (SEC-4.3), (c) encryption at rest (SEC-3.1), (d) access controls (SEC-2.1). Likelihood is Rare because (a) Katakri facility security is stringent, (b) cloud provider is PiTuKri-compliant, (c) multi-region deployment reduces single-point-of-failure. Impact is Catastrophic because classified data breach could compromise national security and result in government shutdown of system.
PR-011		2 (Unlikely)	2 (Minor)	4	Medium		

	Aggregate reach metrics de-anonymized via correlation with public data					Data Flow dataInvento-ry (aggregate metrics); Spec section 4.3 (sensitive data)	Aggregate reach metrics (e.g., "X installs per municipality per day") are published as anonymized aggregates. Risk is that aggregates are de-anonymized via correlation with public data (e.g., municipal population statistics, mobile carrier coverage maps). Likelihood is Unlikely because (a) aggregation is at municipality level (large group size), (b) temporal granularity is daily (not hourly), (c) no unique identifiers are included. Impact is Minor because de-anonymiza-tion would reveal municipali-ty-level install rates (not individual user data).
PR-012	Operator console compro-mised via malware on hardened workstation	2 (Unlikely)	4 (Major)	8	Medium	Data Flow TB-3 (Operator Console boundary); Spec section 5.2 (authentica-tion & access)	Operator console is served only inside Hätäkeskus-laitos internal network (not internet-ex-posed). Risk is that console is compro-mised via malware on operator workstation. Mitigations:

							(a) hardened workstations with endpoint protection, (b) smart card authentication (SEC-1.3), (c) session timeout (SEC-1.4), (d) audit logging (ARC-6.5). Likelihood is Unlikely because (a) workstations are hardened, (b) network is isolated, (c) operator training on security awareness. Impact is Major because console compromise could enable false alert dispatch or incident data manipulation. Confidence is Medium because workstation security details are not fully specified.
PR-013	Ministry dashboard compromised via Virtu/Suomi.fi SSO token theft	2 (Unlikely)	3 (Moderate)	6	High	Data Flow TB-4 (Public Internet to Core Platform); Spec section 5.2 (authentication & access)	Ministry dashboard authentication relies on Virtu/Suomi.fi SSO (SAML 2.0 / OIDC). Risk is that SSO token is stolen via phishing or network attack. Mitigations: (a) MFA required (SEC-1.3), (b) short token lifetime

							(SEC-1.4), (c) HTTPS/TLS (SEC-3.2), (d) read-only scope (SEC-2.1). Likelihood is Unlikely because (a) MFA is strong, (b) tokens are short-lived, (c) Virtu/Suomi.fi is government-operated and secure. Impact is Moderate because token compromise would grant read-only access to audit logs and metrics (not data modification).
PR-014	Citizen app compromised via supply-chain attack (e.g., dependency vulnerability)	2 (Unlikely)	4 (Major)	8	Medium	Spec section 5.3 (technology stack); Architecture section on security scanning	Citizen app is native Swift (iOS) and Kotlin (Android). Risk is that app is compromised via supply-chain attack (e.g., vulnerable dependency, malicious library). Mitigations: (a) dependency vulnerability scanning (SDLC-3.2), (b) SBOM generated for each release (SCS-1.1), (c) code signing and integrity verification, (d) app store review process (Apple/Google). Likelihood is

							Unlikely because (a) native apps have smaller dependency footprint than cross-platform frameworks, (b) scanning is automated, (c) app stores provide additional review. Impact is Major because compromised app could harvest device tokens or location data from millions of users. Confidence is Medium because app build/release process is not fully detailed.
PR-015	Data minimization principle violated if future phases add unnecessary data collection (e.g., precise GPS, user profiling)	3 (Possible)	3 (Moderate)	9	Low	Spec section 3.3 (out of scope); Architecture section on data model	Specification explicitly states that precise GPS is NOT retained and no user profiling is performed. Risk is that Phase 2+ development adds unnecessary data collection to support new features (e.g., cell broadcast targeting, personalized alerts). Likelihood is Possible because (a) feature creep is common, (b) future developers

					may not be aware of privacy constraints, (c) no hard technical barrier prevents data collection. Impact is Moderate because unnecessary data collection would violate GDPR Article 5(1)(c) (data minimization) and require new DPIA. Confidence is Low because Phase 2+ requirements are not specified.

Risk Clustering and Patterns

High-Score Risks (Score >= 12):

- PR-001: SQL injection / API abuse (Score 12) — API security is critical path
- PR-005: Data subject rights process failure (Score 9, but trending High) — Process must be robust

Medium-Score Risks (Score 6-9):

- PR-002, PR-003, PR-006, PR-008, PR-012, PR-013, PR-014, PR-015: Various data access and process risks

Low-Score Risks (Score < 6):

- PR-004, PR-007, PR-009, PR-010, PR-011: Rare events or minor impacts

Risk Themes:

1. **API Security** (PR-001): Internet-exposed API is primary attack surface
2. **Cross-Border Transfer** (PR-006): APNs/FCM transfers require ongoing safeguard verification
3. **Data Retention** (PR-007): Automated deletion must be tested and verified
4. **Process Compliance** (PR-005, PR-009): Manual processes are error-prone
5. **Future Scope Creep** (PR-015): Data minimization principle must be enforced across phases
6. **Supply Chain** (PR-014): Dependencies and build process are attack vectors

Approval Decision and Recommendations

Executive Summary

Hälytin is a critical national air-threat warning system that processes personal data of Finnish residents to deliver life-saving emergency alerts. The DPIA has identified 15 privacy risks ranging from Low to Critical, with residual risks after mitigation clustering in the Low to Medium range. The system implements privacy-by-design principles (anonymous device data, coarse location, no profiling) and comprehensive technical controls aligned with GDPR and Finnish data protection law.

Overall Recommendation: GO WITH CONDITIONS

Hälytin may proceed to Phase 1 MVP launch subject to specific pre-launch conditions outlined below. No fundamental redesign is required. The residual privacy risks are acceptable given the vital-interest purpose (life-saving alerts) and the comprehensive mitigation measures in place.

Risk Summary

Priority	Count	Risk IDs	Residual Score Range
Critical	0	—	—
High	0	—	—
Medium	6	PR-001, PR-005, PR-008, PR-012, PR-013, PR-014	6-9
Low	9	PR-002, PR-003, PR-004, PR-006, PR-007, PR-009, PR-010, PR-011, PR-015	2-5
Total	15		

Residual Risk Profile:

- **Critical**: 0 (0%)
- **High**: 0 (0%)
- **Medium**: 6 (40%)
- **Low**: 9 (60%)

Interpretation: After mitigation, no risks remain at Critical or High severity. 40% of risks are Medium-severity (manageable with ongoing monitoring); 60% are Low-severity (acceptable residual risk). This profile is appropriate for a privacy-critical emergency response system.

Approval Decision

Recommendation: GO WITH CONDITIONS

Hälytin may proceed to Phase 1 MVP launch subject to the following conditions:

Condition 1: DPO Review and Sign-Off (Critical Path)

Requirement: This DPIA must be reviewed and approved by a qualified Data Protection Officer (external, if Hätäkeskuslaitos does not have an internal DPO) before system launch.

Justification: GDPR Article 35(2) requires DPO involvement in DPIA processes. The DPO's written advisory opinion provides independent verification that the DPIA meets regulatory standards.

Timeline: DPO review must be completed and signed off before Phase 1 MVP launch (target: June 2026).

Owner: Hätäkeskuslaitos Legal & Compliance; DPO (external if needed).

Verification: Written DPO approval letter retained in DPIA record.

Condition 2: API Security Hardening (Critical Path)

Requirement: Implement all mitigations for PR-001 (SQL injection / API abuse) before launch:

- Input validation and sanitization on all endpoints (SEC-6.1)
- Parameterized queries for all database operations (SDLC-5.3)
- Rate limiting per client (SEC-6.2)
- WAF on all public endpoints (SEC-4.2)
- API response filtering (SEC-6.5)
- SAST scanning in CI/CD (SDLC-3.1)

Justification: PR-001 is the highest-residual-score Medium-severity risk (Score 12 ’ 6 after mitigation). API is internet-exposed and is the primary attack surface. API security is essential to prevent unauthorized access to device tokens.

Timeline: All mitigations must be implemented and verified before Phase 1 MVP launch.

Owner: Security team; Engineering lead.

Verification: Quarterly penetration testing includes API injection testing; OWASP Top 10 coverage required.

Condition 3: Data Subject Rights Automation (Critical Path)

Requirement: Implement automated data subject rights handling before launch:

- "Export My Data" feature in citizen app (PR-005)
- "Delete My Data" feature in citizen app (PR-005)
- SLA monitoring and escalation process (PR-005)
- Automated request logging and audit trail (PR-005)

Justification: PR-005 (data subject rights process failure) is Medium-severity (Score 9). Automation reduces process failure risk and ensures GDPR Article 12 compliance (30-day response timeline).

Timeline: All features must be implemented and tested before Phase 1 MVP launch.

Owner: Product team; Engineering lead.

Verification: Monthly SLA report; quarterly compliance audit.

Condition 4: Cross-Border Transfer Documentation (Critical Path)

Requirement: Complete and document Transfer Impact Assessment (TIA) for APNs and FCM transfers before launch:

- Assess legal framework of USA for data protection adequacy
- Verify Standard Contractual Clauses (SCCs) are in place with Apple and Google
- Document supplementary measures (encryption, pseudonymization, no profiling)
- Assess residual risk and determine acceptability

Justification: PR-006 (cross-border transfer risks) is Medium-severity (Score 8). Device tokens are transferred to APNs/FCM (USA) for push notification delivery. TIA is required under GDPR Chapter V and EDPB Recommendations 01/2020.

Timeline: TIA must be completed before Phase 1 MVP launch.

Owner: DPO; Legal team.

Verification: Quarterly TIA review; annual legal assessment of USA legal framework.

Condition 5: Facility Security Compliance (Critical Path)

Requirement: Verify Katakri facility security compliance at Hätäkeskuslaitos and cloud provider before launch:

- Hätäkeskuslaitos facilities assessed against Katakri F-series (DEF-SEC-3.1 through DEF-SEC-3.6)
- Cloud provider assessed for PiTuKri compliance
- Facility security clearance from Suojelupoliisi (Facility Security Clearance — FSC)
- Physical security zone model documented and verified

Justification: PR-010 (facility security breach) is Critical-score (Score 5) but low-likelihood after mitigation. Facility security compliance is a hard requirement for handling classified FDF data (TL III).

Timeline: FSC must be obtained before Phase 1 MVP launch. Traficom PiTuKri assessment must be completed before launch. (Note: FSC processing is ~12 months; this is a critical-path dependency that must start immediately.)

Owner: Facility security; Infrastructure team; Suojelupoliski (FSC); Traficom (PiTuKri).

Verification: FSC certificate retained; annual facility security audit.

Condition 6: Privacy Notice Localization (High Priority)

Requirement: Finalize privacy notice in Finnish, Swedish, and English before launch:

- Privacy notice text reviewed for legal accuracy by legal counsel
- Translations reviewed by native speakers

- UI testing for comprehensibility with target population
- Accessibility testing (WCAG 2.2 AA)
- Mandatory onboarding flow enforces notice display and acknowledgment

Justification: PR-009 (privacy notice failure) is Medium-severity (Score 6). Privacy notice is the primary mechanism for informing data subjects of processing activities and rights (GDPR Article 13).

Timeline: Privacy notice must be finalized and tested before Phase 1 MVP launch.

Owner: Product team; Legal team; UX team.

Verification: Monthly notice display verification; annual notice audit.

Condition 7: Operator Training on Data Subject Rights (Medium Priority)

Requirement: Develop and deliver training to Hätäkeskuslaitos operators on data subject rights handling before launch:

- Training covers GDPR data subject rights (access, erasure, portability, restriction, object)
- Training covers Hälytin-specific rights request processes
- Training includes hands-on practice with rights request workflows
- Training completion tracked and verified

Justification: Operators will handle data subject rights requests (especially from Sisäministeriö officials). Operator training ensures consistent and compliant rights handling.

Timeline: Training must be completed before Phase 1 MVP launch.

Owner: DPO; Hätäkeskuslaitos Training team.

Verification: Training completion certificates retained; annual refresher training.

Condition 8: Data Processor Agreements (Medium Priority)

Requirement: Execute data processor agreements with all third-party processors before launch:

- Cloud provider (data hosting, encryption, backup)
- Apple (APNs data processing)
- Google (FCM data processing)
- Mobile carriers (SMS gateway data processing)
- Yleisradio (broadcast trigger)

Justification: GDPR Article 28 requires written data processor agreements with all processors. Agreements must include data protection obligations, sub-processor authorization, data subject rights support, and audit rights.

Timeline: All processor agreements must be executed before Phase 1 MVP launch.

Owner: Legal team; DPO.

Verification: Processor agreements retained in contract repository; annual processor compliance audit.

Condition 9: Audit Log Integrity Verification (Medium Priority)

Requirement: Implement and verify cryptographic audit log integrity before launch:

- Each audit entry includes hash of previous entry (cryptographic chain)
- Tamper detection implemented (any modification breaks chain)
- Audit log immutability enforced at database level
- Audit log exports signed and timestamped
- Monthly integrity verification test

Justification: Audit logs are the backbone of accountability for a critical emergency response system. Cryptographic chaining ensures tamper-evidence and enables post-incident reconstruction of alert chain.

Timeline: Audit log integrity must be implemented and tested before Phase 1 MVP launch.

Owner: Engineering team; Security team.

Verification: Monthly integrity verification test; annual audit log security assessment.

Condition 10: Quarterly Privacy Risk Review (Ongoing)

Requirement: Conduct quarterly privacy risk reviews during Phase 1 MVP operation (minimum 4 reviews before Phase 2 decision):

- Review privacy risk register for new risks
- Verify mitigation measures are effective
- Update risk scores based on operational experience
- Escalate any new High or Critical risks to leadership
- Document findings and recommendations

Justification: Privacy risks evolve as the system operates. Quarterly reviews ensure risks remain within acceptable levels and mitigations remain effective.

Timeline: First review 30 days post-launch; subsequent reviews quarterly.

Owner: DPO; Security team.

Verification: Quarterly risk review reports retained; escalation log maintained.

Conditions Summary Table

Condition	Priority	Deadline	Owner	Verification

1. DPO Sign-Off	Critical	Before launch	DPO	Written approval letter
2. API Security Hardening	Critical	Before launch	Security team	Penetration test results
3. Data Subject Rights Automation	Critical	Before launch	Product team	Feature testing + SLA monitoring
4. Cross-Border Transfer Documentation	Critical	Before launch	DPO + Legal	TIA document + SCC copies
5. Facility Security Compliance	Critical	Before launch	Facility security	FSC certificate + PiTuKri assessment
6. Privacy Notice Localization	High	Before launch	Legal + Product	Notice testing report
7. Operator Training	High	Before launch	DPO + Training	Training completion certificates
8. Data Processor Agreements	High	Before launch	Legal	Signed processor agreements
9. Audit Log Integrity	Medium	Before launch	Engineering	Integrity verification test report
10. Quarterly Privacy Risk Review	Ongoing	Every 90 days	DPO	Quarterly risk review reports

Conditions Not Required

The following measures are recommended best practices but are NOT required as launch conditions:

- **Supervisory authority prior consultation** (Article 36): Not required because residual risks are not High or Critical. However, notification to Tietosuojavaltuutettu is recommended after launch.
- **Phase 2 feature design review**: Deferred to Phase 2 launch gate; not required for Phase 1 MVP.
- **Supply-chain security assessment**: Recommended but not required if dependency scanning and SBOM are in place.
- **User privacy survey**: Recommended post-launch; not required before launch.

Conditions Rationale

Why these conditions?

1. **DPO Sign-Off**: Regulatory requirement (GDPR Article 35(2)); independent verification.
2. **API Security**: Highest-residual-score Medium risk; internet-exposed attack surface.
3. **Data Subject Rights**: Core GDPR compliance; process failure would violate Article 12.
4. **Cross-Border Transfers**: Mandatory GDPR Chapter V compliance; ongoing legal risk.
5. **Facility Security**: Hard requirement for classified data handling (Katakri, FSC).
6. **Privacy Notice**: Core transparency requirement; failure would violate Article 13.
7. **Operator Training**: Ensures consistent rights handling; critical for operator-facing processes.
8. **Data Processor Agreements**: Mandatory GDPR Article 28 requirement; legal risk if missing.
9. **Audit Log Integrity**: Essential for post-incident accountability; enables chain-of-custody verification.
10. **Quarterly Reviews**: Ongoing risk management; catches emerging risks early.

Conditions Not Met = No-Go

If any of the 5 Critical-priority conditions (1, 2, 3, 4, 5) are not met before launch, the system must not proceed to production. Proceeding without these conditions would violate GDPR and expose Hätäkeskuslaitos to regulatory enforcement action.

If any of the 4 High-priority conditions (6, 7, 8) are not met, launch may be delayed up to 30 days to remediate. If remediation is not feasible within 30 days, escalate to Hätäkeskuslaitos Director General and Sisäministeriö for risk acceptance decision.

Monitoring and Review Schedule

Phase 1 MVP Launch Gate (June 2026)

- Verify all 10 conditions are met
- DPO final sign-off
- Go/No-Go decision by Hätäkeskuslaitos and Sisäministeriö

Post-Launch Monitoring (July 2026 - June 2027)

- Monthly privacy incident report
- Quarterly privacy risk review
- Quarterly penetration testing (API security)
- Quarterly SLA monitoring (data subject rights)
- Annual DPIA review and update

Phase 2 Decision Gate (June 2027)

- Full DPIA review and update for Phase 2 features
- New privacy risks identified and assessed
- New conditions imposed if necessary
- Go/No-Go decision for Phase 2 launch

Escalation Procedures

If any condition cannot be met or any new High/Critical risk emerges during implementation:

1. **Identify issue**: Security team or DPO identifies unmet condition or new risk
2. **Notify leadership**: Escalate to Hätäkeskuslaitos Director General and Sisäministeriö Preparedness Director within 24 hours
3. **Risk assessment**: Conduct rapid risk assessment; determine if launch delay is necessary
4. **Remediation planning**: Develop remediation plan with timeline and owner
5. **Decision**: Leadership decides to (a) delay launch to remediate, (b) proceed with documented risk acceptance, or (c) redesign system
6. **Documentation**: All escalations and decisions documented in DPIA record

Approval Signatures

This DPIA requires approval and sign-off from:

Role	Organization	Approval Required	Timeline
Data Protection Officer	External DPO or Hätäkeskuslaitos	Yes	Before launch
Legal Counsel	Hätäkeskuslaitos Legal & Compliance	Yes	Before launch
Information Security Officer	Hätäkeskuslaitos Information Security	Yes	Before launch
Director General	Hätäkeskuslaitos	Yes	Before launch
Preparedness Division Director	Sisäministeriö	Yes	Before launch
Program Steering Group Chair	Sisäministeriö	Yes	Before launch

Conclusion

Hälytin is a critical emergency response system designed with privacy-by-design principles and comprehensive technical controls. The DPIA has identified 15 privacy risks, none of which are Critical or High after mitigation. The system aligns with GDPR principles and Finnish data protection law. Subject to the 10 conditions outlined above, Hälytin may proceed to Phase 1 MVP launch.

The conditions are designed to ensure that:

1. All Critical privacy risks are mitigated before launch
2. Regulatory requirements (GDPR, Katakri, PiTuKri) are met
3. Data subject rights are supported through automated processes
4. Accountability and audit trails are in place
5. Ongoing monitoring and review processes are established

Recommendation: APPROVE WITH CONDITIONS

Hälytin may proceed to Phase 1 MVP launch upon satisfaction of all 10 conditions, with particular emphasis on the 5 Critical-priority conditions (DPO sign-off, API security, data subject rights automation, cross-border transfer documentation, facility security compliance).

DPIA Document Status: FINAL (pending DPO review and approval)

DPIA Review Date: June 2026 (Phase 1 MVP launch gate)

DPIA Update Trigger: Material change to processing activities; new personal data collection; new external integrations; any High or Critical privacy risk; supervisory authority guidance or regulatory changes

DPIA Owner: Data Protection Officer (Hätäkeskuslaitos or external consultant)

DPIA Custodian: Hätäkeskuslaitos Legal & Compliance

Data Subject Rights Implementation

Hälytin supports all GDPR data subject rights through documented processes and technical mechanisms. Response timelines comply with GDPR Article 12 (30-day default; one-month extension for complex cases).

Data Subject Rights Summary

Right	Article	Implementation	Response Time	Automated	Verification
Right of Access	15	Citizen app includes "Export My Data" feature; downloads all registered device data (token hash, location, language, accessibility flags, install timestamp) in machine-readable JSON format; operator/ministry officials access audit logs via read-only dashboard (time-range filters, export to CSV)	30 days (citizen data typically <1 day; audit logs may require 5-10 days due to export volume)	Partially (citizen data auto-generated; audit exports require manual filtering by role)	User identity verified via app session for citizens; SSO token for officials
Right to Rectification	16	Citizen app allows users to update language preference and accessibility flags in real-time; device location cannot be rectified (it is derived from registration, not stored as user-provided fact); operator/ministry roles cannot be rectified by data subject (managed by Hätäkeskuslaitos HR)	Real-time for citizen-updatable fields; N/A for derived/HR-managed fields	Yes (citizen app updates propagate immediately to database)	User identity verified via app session
Right to Erasure	17	Citizen app includes "Delete My Data" button; triggers immediate cascading deletion of device token, location, metadata, install timestamp from all data stores; hashed token retained for 90 days post-deletion to prevent re-registration spam (justified under Art. 17(3)(b) — necessary for spam	Real-time for citizen device data (deletion confirmation within 24 hours); N/A for operator/audit data	Yes (citizen deletion triggers automated background job)	User identity verified via app session; confirmation email sent to registered email (if available)

		prevention); operator/ministry staff cannot request erasure of their own identity (retained for accountability); audit logs cannot be deleted before retention minimum (justified under Art. 17(3)(d) — legal obligation)			
Right to Data Portability	20	Citizen app includes "Export My Data" feature; downloads all personal data in machine-readable JSON format (device metadata, language preference, accessibility flags, install timestamp); data is portable (no proprietary format); operator/ministry data is not portable (not collected on basis of consent or contract; Art. 20(1) exclusion)	30 days (typically <1 day)	Yes (auto-generated on-demand)	User identity verified via app session
Right to Restriction	18	Citizen app allows users to toggle notification permissions on/off; when restricted, device remains registered but receives no alerts (equivalent to temporary suspension); users can lift restriction at any time; operator/ministry data cannot be restricted (necessary for ongoing accountability)	Real-time (permission toggle is immediate)	Yes (device flag updated immediately)	User identity verified via app session
Right to Object	21	Citizen app includes "Opt Out" option; equivalent to uninstall + deletion; users can object to all processing except vital-interest alerts (Art. 21(1) exception — vital interests override right to object); users can object to operator/audit logging (not applicable —	Real-time (opt-out is immediate)	Yes (device deletion triggered immediately)	User identity verified via app session

		they don't have choice in this processing)			
Right to Not Be Subject to Automated Decision-Making	22	Hälytin does not perform automated decision-making with legal or significant effects on individuals; alert dispatch is deterministic (geography-based, not profiling-based); no credit decisions, hiring decisions, or other consequential automated decisions are made	N/A	N/A	N/A
Right to Lodge a Complaint	77	Privacy notice provided during onboarding includes contact details of Tietosuojavaltuutettu (Finnish Data Protection Ombudsman); citizens can lodge complaints directly with the ombudsman; Hälytin provides a contact form for privacy concerns (routed to DPO)	N/A (complaint goes to ombudsman, not Hälytin)	Hälytin confirms receipt of privacy concerns within 5 business days	N/A

Detailed Implementation Descriptions

Right of Access (Article 15)

For Citizen Users:

- Citizen app includes an "Account" section with "Export My Data" button
- Button triggers immediate download of all personal data in machine-readable JSON format
- Data includes: device token (hashed), platform, coarse location (municipality code), language preference, accessibility flags, install timestamp, revocation status (if applicable)
- No data is omitted; no redactions applied
- Confirmation email sent to user (if email was collected during onboarding)

For Operators and Ministry Officials:

- Core API includes `/v1/audit-entries` endpoint (administrator and ministry_official roles only)
- Endpoint supports filtering by date range, entity type, actor ID, action type
- Response includes full audit log entry details (entity, action, actor, timestamp, payload)
- Exports available in JSON and CSV formats

- Queries are logged and audited

Response Process:

- Citizen request: auto-generated, typically delivered within 1 day
- Operator/ministry request: manual review by DPO or data controller, typically 5-10 days for large date ranges
- Complex requests (multiple date ranges, large exports): up to 30 days

Right to Rectification (Article 16)

For Citizen Users:

- Citizen app includes "Settings" section where users can update:
  - Language preference (FI / SV / EN)
  - Accessibility flags (high contrast, large type, vibration-only mode)
- Updates are applied immediately to the database
- Confirmation message displayed in app
- Device location cannot be rectified (it is derived from device registration, not user-provided fact)
- Device token cannot be rectified (it is generated by the device OS, not user-provided)

For Operators and Ministry Officials:

- Operator roles and certification status are managed by Hätäkeskuslaitos HR system
- Rectification requests must go through HR, not through Hälytin
- Data controller (Hätäkeskuslaitos) coordinates with HR to update identity provider records

Response Process:

- Citizen updates: real-time (changes visible immediately)
- Operator updates: coordinated with HR; typically 5-10 business days

Right to Erasure (Article 17)

For Citizen Users:

- Citizen app includes "Delete My Data" button in Settings
- Button triggers immediate deletion of:
  - Device token (raw encrypted form)
  - Device token (hashed form) — retained for 90 days only (justified under Art. 17(3)(b) — necessary to prevent re-registration spam attacks)
  - Coarse location (municipality code)
  - Language preference
  - Accessibility flags
  - Install timestamp

- Deletion is cascading: all related records in PostgreSQL, Valkey cache, and object storage are deleted
- Deletion is irreversible: no recovery from backups
- Confirmation email sent to user
- Device is marked as revoked; cannot re-register for 90 days (spam prevention)

Grounds for Deletion:

- Data is no longer necessary for the purpose (user uninstalled app)
- Data subject withdraws consent (not applicable; vital interests basis does not require consent)
- Data subject objects to processing (Art. 21)
- Retention period expired (device data: upon uninstall; audit logs: 10 years minimum)

Exceptions to Deletion (Art. 17(3)) — Deletion is NOT required for:

- Audit log entries (Art. 17(3)(d) — legal obligation to retain for accountability)
- Operator identity records (Art. 17(3)(d) — legal obligation to retain for accountability)
- Hashed device token (90 days post-deletion) — Art. 17(3)(b) — necessary to prevent spam

Response Process:

- Citizen deletion: real-time (data deleted within 24 hours; confirmation email within 24 hours)
- Audit log deletion requests: declined with explanation of legal retention obligation

Right to Data Portability (Article 20)

Scope:

- Applies only to citizen device data (collected on basis of vital interests, which does not trigger portability right per Art. 20(1)(a))
- However, Hälytin voluntarily supports portability as a privacy-enhancing feature
- Operator and audit data are excluded (not collected on basis of consent or contract)

Implementation:

- Citizen app includes "Export My Data" feature (same as right of access)
- Data is provided in machine-readable JSON format
- Data includes all personal data elements (device token hash, location, language, accessibility flags, timestamp)
- Data can be ported to another emergency alert system if desired

Response Process:

- Auto-generated, typically within 1 day
- Download link sent to user (if email available)

Right to Restriction (Article 18)

Implementation:

-

Citizen app includes notification permission toggle (separate from app uninstall)

- When notifications are disabled, device remains registered but receives no alerts
- Device can be re-enabled at any time by toggling notifications back on
- Equivalent to temporary suspension without data deletion

Grounds for Restriction:

- Data subject contests accuracy of data (Art. 18(1)(a)) — not applicable; device data is not "accurate/inaccurate" (it is derived from device OS)
- Processing is unlawful (Art. 18(1)(b)) — data subject can request restriction while controller verifies legality
- Data is no longer necessary (Art. 18(1)(c)) — user can disable notifications if they no longer want alerts
- Data subject objects to processing (Art. 18(1)(d)) — user can disable notifications pending verification of legitimate interests (not applicable; vital interests override)

Response Process:

- Real-time: notification toggle is immediate
- Device marked as "restricted" in database
- No alerts sent while restricted
- Restriction can be lifted at any time by user

Right to Object (Article 21)

Scope:

- Citizens can object to all processing except vital-interest alerts (Art. 21(1) exception — vital interests override right to object)
- Equivalent to uninstall + data deletion
- Operators cannot object to their own audit logging (necessary for accountability; legal obligation)

Implementation:

- Citizen app includes "Opt Out" button (equivalent to delete + uninstall)
- Clicking "Opt Out" triggers same deletion process as "Delete My Data"
- Device is marked as opted-out; cannot re-register for 90 days

Response Process:

- Real-time: opt-out is immediate
- Confirmation email sent to user

Right to Not Be Subject to Automated Decision-Making (Article 22)

Scope:

- Hälytin does not perform automated decision-making with legal or significant effects on individuals
- Alert dispatch is deterministic and rule-based (geography-based, not profiling-based)
-

No credit decisions, hiring decisions, or other consequential automated decisions

Implementation:

- Article 22 is not applicable to Hälytin
- All alert dispatch decisions are based on FDF threat object (human-confirmed by operators) and geographic targeting (deterministic, not profiling-based)

Right to Lodge a Complaint (Article 77)

Implementation:

- Privacy notice provided during app onboarding includes contact details of Tietosuojavaltuutettu (Finnish Data Protection Ombudsman)
- Citizen app includes "Privacy" section with link to ombudsman contact form
- Hälytin provides a privacy concern form (in-app contact form) that routes to DPO
- DPO responds to privacy concerns within 5 business days
- All complaints are logged and tracked

Data Subject Rights Request Process

Citizen User Request Process:

1. User initiates request via citizen app ("Export My Data", "Delete My Data", "Opt Out") or via halytin.fi contact form
2. User identity verified via app session or email confirmation
3. Request is logged in audit system
4. Request is processed according to right-specific procedure (see above)
5. Confirmation email sent to user (if email available)
6. Request completion time tracked and monitored for SLA compliance (30 days)

Operator/Ministry Official Request Process:

1. Request submitted via privacy concern form or direct email to DPO
2. Request identity verified (email domain check for ministry officials; HR record check for operators)
3. Request is logged and tracked
4. DPO determines if request is valid and applicable
5. Data controller (Hätäkeskuslaitos) approves request
6. Request is processed according to right-specific procedure
7. Response sent to requester within 30 days

Request Tracking:

- All requests logged in audit system with timestamp, requester identity, request type, response time
- Monthly reporting to DPO on request volume and response time metrics
- Non-compliance flagged for escalation

Denial of Requests

Requests may be denied or partially denied in the following circumstances:

Reason	Applicable Right	Response
Request is manifestly unfounded or excessive	All	Deny; explain why; offer alternative
Request seeks to verify accuracy of device-derived data	Rectification, Erasure	Explain that data is derived, not user-provided; offer alternative (e.g., re-registration)
Request seeks to delete audit logs before retention minimum	Erasure	Deny; explain legal retention obligation; offer redaction alternative (if applicable)
Request seeks to delete operator identity before retention minimum	Erasure	Deny; explain legal obligation for accountability; offer anonymization alternative (if applicable)
Request seeks to port audit log data	Portability	Deny; explain that audit logs are not portable (legal obligation basis); offer access alternative
Request seeks to restrict vital-interest alerts	Restriction, Objection	Deny; explain vital-interest exception; offer alternative (disable notifications)

Accessibility of Rights

- All rights requests are available in Finnish, Swedish, and English
- Citizen app includes accessible UI for rights requests (WCAG 2.2 AA compliant)
- Contact forms include text-to-speech and screen-reader support
- Response communications are provided in the language requested by data subject
- No fees charged for rights requests (except manifestly unfounded/excessive requests may incur cost recovery)

Compliance Verification

- Quarterly audit of rights request handling (sample 10% of requests; verify response time, accuracy, completeness)
- Annual reporting to DPO on rights request metrics
- External audit by accredited body (as part of Katakri/PiTuKri assessment)
- Data subject satisfaction survey (annual)

Mitigation Measures

This section describes technical and organizational controls to mitigate the privacy risks identified in Section 4. Each mitigation is mapped to specific risks, policy controls, and residual risk levels.

Mitigation Strategy Summary

Risk ID	Primary Risk	Mitigation Strategy	Control Type	Timeline	Owner
PR-001	SQL injection / API abuse	Input validation, parameterized queries, rate limiting, WAF	Technical + Organizational	Phase 1 MVP	Security team
PR-002	Unauthorized database access	Encryption at rest, least-privilege access, network segmentation	Technical	Phase 1 MVP	Infrastructure team
PR-003	TLS misconfiguration	Certificate pinning, TLS enforcement, security scanning	Technical	Phase 1 MVP	Security team
PR-004	Unauthorized location collection	Code review, static analysis, runtime monitoring	Technical + Organizational	Phase 1 MVP	Engineering lead
PR-005	Data subject rights delays	Automated request handling, SLA monitoring, escalation process	Organizational	Phase 1 MVP	DPO
PR-006	Cross-border transfer risks	Transfer Impact Assessment, SCCs, supplementary measures	Organizational + Legal	Phase 1 MVP	DPO + Legal
PR-007	Data retention beyond necessary period	Automated deletion, backup policy, retention verification	Technical + Organizational	Phase 1 MVP	Database team
PR-008	RBAC bypass	Multi-layered access control, code review, security scanning	Technical	Phase 1 MVP	Security team
PR-009	Privacy notice failure	Mandatory onboarding flow, UI testing, localization QA	Organizational	Phase 1 MVP	Product team
PR-010	Facility security breach	Katakri compliance, physical security, network segmentation	Technical + Organizational	Phase 1 MVP	Facility security
PR-011	De-anonymization via correlation	Aggregation at municipality level, temporal granularity, no unique IDs	Technical	Phase 1 MVP	Data team
PR-012			Organizational	Phase 1 MVP	Hätäkeskuslaitos IT

	Operator console malware	Hardened workstations, endpoint protection, session timeout			
PR-013	SSO token theft	MFA, short token lifetime, HTTPS/TLS, read-only scope	Technical	Phase 1 MVP	Security team
PR-014	Supply-chain attack	Dependency scanning, SBOM, code signing, app store review	Technical	Phase 1 MVP	Build team
PR-015	Data minimization violation in Phase 2+	Architecture review, privacy review gate, DPIA update process	Organizational	Ongoing	DPO

Detailed Mitigation Descriptions

PR-001: SQL Injection / API Abuse

Risk: Unauthorized access to device tokens via SQL injection or API abuse; Score 12 (High)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Input validation and sanitization on all API endpoints	Technical	SEC-6.1, SDLC-5.1	All endpoints validate input against schema; reject non-conforming input with 400 error; log rejected inputs for security monitoring
Parameterized queries / prepared statements	Technical	SDLC-5.3	All database queries use parameterized queries; no string concatenation; ORM with query escaping
Rate limiting per client	Technical	SEC-6.2	Device registration: 10 requests/minute per IP, 1 request/device token per 24 hours; operator console: 60 requests/minute per session; ministry dashboard: 120 requests/minute per session
WAF on all public endpoints	Technical	SEC-4.2, SEC-4.5	Cloud-native WAF blocks common injection patterns (SQL, XSS, command injection); rules updated weekly
API response filtering	Technical	SEC-6.5	API responses never include stack traces, internal implementation details, or raw error messages; generic error messages returned to client
Security scanning in CI/CD	Technical	SDLC-3.1	SAST on every pull request; dependency scanning; secret detection; results reviewed before merge

Residual Risk: Score 6 (Medium) — Parameterized queries and WAF eliminate most injection risk; residual risk from zero-day vulnerabilities or novel attack patterns.

Verification: Quarterly penetration testing includes API injection testing; OWASP Top 10 coverage required.

PR-002: Unauthorized Database Access

Risk: Unauthorized access to coarse location data via database compromise; Score 8 (Medium)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
AES-256 encryption at rest	Technical	SEC-3.1, DEF-SEC-2.1	All data stores (PostgreSQL, Valkey, object storage) encrypted with AES-256; customer-controlled keys via Finnish sovereign KMS
Least-privilege database access	Technical	SEC-2.1, SEC-2.5	Core API has INSERT/UPDATE/DELETE on device table only; Alert Dispatch Service has SELECT-only on device table; separate database roles for each service; service accounts documented with owners
Network segmentation	Technical	SEC-4.3, DEF-SEC-1.3	Database is not internet-exposed; access only from Core API via TLS; network firewall rules enforce this
Encrypted database connections	Technical	SEC-3.5	All connections to PostgreSQL use TLS 1.2+; certificate pinning for internal connections
Database activity monitoring	Technical	DEF-SEC-1.4	Real-time monitoring of database queries; anomalous queries (e.g., SELECT * FROM device) trigger alerts; logs retained for 2 years
Backup encryption and access control	Technical	OPS-5.3	Backups encrypted at rest; backup access restricted to infrastructure team; restore operations logged and audited

Residual Risk: Score 4 (Low) — Encryption and network segmentation eliminate most database compromise risk; residual risk from insider threat or sophisticated nation-state attack.

Verification: Annual penetration testing includes database security assessment; access logs audited monthly.

PR-003: TLS Misconfiguration

Risk: Device tokens transmitted in plaintext to APNs/FCM due to TLS misconfiguration; Score 4 (Low)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
TLS 1.3 for all external connections	Technical	SEC-3.2, TIC-7.1	All outbound connections use TLS 1.3; TLS 1.2 minimum for fallback; no plaintext connections
Certificate pinning for APNs	Technical	DEF-SEC-2.2	APNs client certificate pinned to FDF CA (for FDF intake); Apple APNs certificate pinned to Apple CA
Automatic certificate renewal	Technical	OPS-2.1	Let's Encrypt certificates renewed automatically 30 days before expiry; renewal failures trigger alerts
TLS configuration scanning	Technical	SDLC-3.4	Infrastructure code scanned for TLS misconfigurations; weak cipher suites rejected; configuration validated in CI/CD
Runtime TLS verification	Technical	OPS-1.5	All outbound connections verified to use TLS at runtime; plaintext connections rejected; verification logged

Residual Risk: Score 2 (Very Low) — TLS enforcement at platform level eliminates most misconfiguration risk; residual risk from cryptographic break or nation-state MITM.

Verification: Quarterly TLS audit; external security scanning (e.g., SSL Labs); certificate pinning tested monthly.

PR-004: Unauthorized Location Collection

Risk: Location privacy violation via continuous GPS tracking if developer implements unauthorized location collection; Score 6 (Medium)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Explicit data minimization requirement in specification	Organizational	DATA-3.7, GDPR Art. 5(1)(c)	Specification explicitly prohibits precise GPS retention; only municipality-level location retained
Code review requirement	Organizational	SDLC-2.2	All code changes to device registration and location handling require security team review; location API calls flagged for review
Static analysis for location APIs	Technical	SDLC-3.1	SAST scans for location API calls (CLLocationManager, FusedLocationProvider); findings reviewed before merge
Runtime monitoring	Technical	OPS-1.5	App runtime monitoring detects location API calls; un-

			expected location access triggers alert
Architecture constraint: no location API in Core API	Technical	ARC-2.2	Core API does not link against location libraries; location must be provided by client app only
Privacy impact assessment for location handling	Organizational	GDPR Art. 35	Any change to location handling requires privacy impact assessment and DPO review

Residual Risk: Score 3 (Low) — Code review and static analysis eliminate most unauthorized collection risk; residual risk from obfuscated code or compromised developer.

Verification: Quarterly code review of location-related functions; runtime monitoring logs reviewed monthly; privacy impact assessment for any location changes.

PR-005: Data Subject Rights Process Failure

Risk: Data subject rights requests denied or delayed due to process failure; Score 9 (Medium-High)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Automated request handling for citizen requests	Technical	GDPR Art. 12	"Export My Data" and "Delete My Data" buttons in app trigger automated processing; no manual review required for standard requests
SLA monitoring and escalation	Organizational	DATA-3.4	All requests tracked with submission date and 30-day deadline; escalation process if deadline at risk; weekly SLA report to DPO
Request logging and audit trail	Technical	ARC-6.5	All requests logged with timestamp, requester identity, request type, response time, outcome; logs retained for 2 years
DPO review of complex requests	Organizational	GDPR Art. 35(2)	Requests involving large exports or sensitive data routed to DPO for review; DPO has 5-day review SLA
Citizen notification of request status	Organizational	GDPR Art. 12	Automatic email confirmation sent on request receipt; status update at 15-day mark if processing; final response sent before 30-day deadline
Annual compliance audit	Organizational	GDPR Art. 5(2)	Annual audit of 10% of requests; verify response time, accuracy, completeness; results reported to DPO

Residual Risk: Score 3 (Low) — Automation and SLA monitoring eliminate most process failure risk; residual risk from system downtime or DPO capacity constraints.

Verification: Monthly SLA report; quarterly compliance audit; annual reporting to DPO.

PR-006: Cross-Border Transfer Risks (APNs/FCM)

Risk: Device tokens transferred to APNs/FCM without adequate safeguards; Score 8 (Medium)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Transfer Impact Assessment (TIA)	Organizational	GDPR Art. 46, EDPB Recommendations 01/2020	Completed TIA for both Apple APNs and Google FCM; assessed legal framework of USA, supplementary measures, enforceability of rights
Standard Contractual Clauses (SCCs)	Legal	GDPR Art. 46(2)(c)	SCCs in place with Apple and Google; modular SCC version; covers all data processing activities
Data pseudonymization	Technical	GDPR Art. 32(1)(a)	Device tokens stored as one-way hash server-side; raw tokens encrypted before transmission; Apple and Google receive tokens only for delivery, not for retention
Supplementary measures	Technical	EDPB Recommendations 01/2020	Encryption in transit (TLS 1.3); no precise location transferred; tokens are short-lived (revoked on uninstall); no profiling or secondary use
Quarterly safeguard verification	Organizational	GDPR Art. 46(2)(c)	Quarterly review of Apple and Google data protection commitments; monitoring of legal changes in USA; updates to TIA as needed
Data subject notification	Organizational	GDPR Art. 13	Privacy notice discloses transfers to USA; explains safeguards (SCCs, encryption, pseudonymization); informs data subjects of rights

Residual Risk: Score 4 (Low) — SCCs, pseudonymization, and supplementary measures provide adequate safeguards; residual risk from US government legal process (FISA, national security orders) or Apple/Google policy change.

Verification: Quarterly TIA review; annual legal assessment of USA legal framework; monitoring of EDPB guidance.

PR-007: Data Retention Beyond Necessary Period

Risk: Device data retained beyond necessary retention period due to backup/archival failure; Score 6 (Medium)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation

Automated deletion on device revocation	Technical	DATA-2.5, GDPR Art. 17	Background job runs hourly; identifies revoked devices; cascades deletion to all data stores (primary DB, cache, backups)
Retention policy enforcement in database	Technical	DATA-2.1	Database policies enforce retention limits; data older than retention period flagged for deletion; automated cleanup job
Backup retention alignment	Organizational	DATA-2.4, OPS-5.2	Backup retention policy mirrors primary data retention; deleted data excluded from new backups; old backups purged on schedule
Deletion verification testing	Organizational	OPS-5.2, SDLC-2.5	Monthly test of deletion process; verify deleted data not recoverable from backups or caches; test results logged
Audit log of all deletions	Technical	ARC-6.5	Every deletion operation logged with timestamp, reason, deleted data count; deletion logs retained for 2 years
Quarterly retention audit	Organizational	DATA-2.2	Quarterly review of data retention; verify no data retained beyond policy; sample 1% of database records

Residual Risk: Score 3 (Low) — Automation and verification testing eliminate most retention risk; residual risk from backup media that cannot be securely destroyed.

Verification: Monthly deletion testing; quarterly retention audit; annual backup media destruction verification.

PR-008: RBAC Bypass

Risk: Operator identity and audit log data accessible to unauthorized persons due to RBAC bypass; Score 8 (Medium)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Multi-layered access control	Technical	SEC-2.6, ARC-6.1	RBAC enforced at application layer; separate database roles for read/write; network-level access control (operator console on internal network only)
Role-based authorization checks	Technical	SEC-2.6	Every API endpoint checks requester role before returning data; authorization failures logged as security events
Least-privilege database roles	Technical	SEC-2.1, SEC-2.5	Separate database roles for Core API (read/write),

			Alert Dispatch Service (read-only), DPO (audit read-only); no wildcard permissions
Code review of authorization logic	Organizational	SDLC-2.2	All authorization code changes require security team review; privilege escalation scenarios tested
Security scanning for authorization bypass	Technical	SDLC-3.1	SAST scans for hardcoded roles, missing authorization checks, insecure direct object references (IDOR); findings reviewed before merge
Audit logging of authorization decisions	Technical	ARC-6.5	All authorization checks logged; failures logged as security events; logs retained for 2 years; monitored for patterns
Quarterly access control audit	Organizational	SEC-2.2	Quarterly review of all role assignments; verify least-privilege is maintained; test authorization bypass scenarios

Residual Risk: Score 4 (Low) — Multi-layered controls and code review eliminate most bypass risk; residual risk from zero-day code injection or insider threat.

Verification: Quarterly access control audit; annual penetration testing includes authorization bypass scenarios; monthly authorization failure log review.

PR-009: Privacy Notice Failure

Risk: Privacy notice inadequate or not provided due to process failure; Score 6 (Medium)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Mandatory onboarding flow	Technical	GDPR Art. 13	Privacy notice is mandatory step in onboarding; users cannot proceed without reading and acknowledging notice
Multi-language support	Technical	DATA-3.2	Privacy notice available in FI, SV, EN; language selection on first app launch
Accessible UI for privacy notice	Technical	WCAG 2.2 AA	Privacy notice text is large, high-contrast, screen-reader-friendly; audio version available
Privacy notice testing	Organizational	SDLC-2.1	Privacy notice tested for comprehensibility; user testing with target population; feedback incorporated
Localization QA	Organizational	SDLC-2.1	All translations reviewed by native speakers; legal review of translations for accuracy;

			localization bugs tracked and fixed
Audit logging of notice acknowledgment	Technical	ARC-6.5	Every user acknowledgment logged with timestamp and app version; acknowledgment records retained for 2 years
Annual notice audit	Organizational	GDPR Art. 13	Annual review of privacy notice; verify notice is still accurate; update if processing changes

Residual Risk: Score 2 (Very Low) — Mandatory onboarding and testing eliminate most notice failure risk; residual risk from user dismissing notice without reading.

Verification: Monthly notice display verification (sample 1% of new installs); annual notice audit; quarterly localization review.

PR-010: Facility Security Breach

Risk: Facility security breach at Hätäkeskuslaitos or cloud provider enabling unauthorized access to classified data; Score 5 (Critical)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Katakri facility security compliance	Organizational	DEF-SEC-3.1 through DEF-SEC-3.6, KATAKRI F-series	Hätäkeskuslaitos facilities assessed against Katakri F-series; physical security zone model (public, controlled, restricted, secure); access control, intrusion detection, CCTV
PiTuKri cloud provider selection	Organizational	PiTuKri v1.1	Cloud provider assessed for PiTuKri compliance; TL III data processing approved; facility security verified
Encryption at rest	Technical	SEC-3.1, DEF-SEC-2.1	All classified data encrypted with AES-256; customer-controlled keys; keys stored separately from data
Network segmentation	Technical	SEC-4.3, DEF-SEC-1.3	FDF intake in isolated DMZ; no outbound connectivity to public internet; network firewall enforces segmentation
Multi-region deployment	Technical	ARC-5.2	Data replicated across two geographically separated Finnish availability zones; failover tested quarterly
Facility security audits	Organizational	KATAKRI I-14	Annual facility security audits by accredited body; findings remediated within 30 days; audit reports retained

Residual Risk: Score 2 (Very Low) — Katakri compliance and encryption eliminate most facility breach risk; residual risk from nation-state physical attack or insider threat.

Verification: Annual facility security audit; quarterly multi-region failover test; annual encryption key rotation verification.

PR-011: De-Anonymization via Correlation

Risk: Aggregate reach metrics de-anonymized via correlation with public data; Score 4 (Low)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Aggregation at municipality level	Technical	GDPR Art. 32(1)(a)	Reach metrics aggregated at municipality (kunta) granularity; no sub-municipal aggregates published
Temporal granularity (daily minimum)	Technical	GDPR Art. 32(1)(a)	Reach metrics aggregated by day; no hourly or sub-hourly aggregates; no per-user temporal tracking
No unique identifiers in aggregates	Technical	GDPR Art. 32(1)(a)	Aggregates include only count and municipality code; no device identifiers, no user identifiers
Minimum cell size enforcement	Technical	GDPR Art. 32(1)(a)	Aggregates suppressed if cell size <10 users; prevents identification of small groups
De-anonymization risk assessment	Organizational	GDPR Art. 32(1)(a)	Quarterly assessment of de-anonymization risk; monitoring of public data sources that could enable correlation
Data publication review	Organizational	GDPR Art. 13	All published aggregates reviewed by DPO before publication; de-anonymization risk assessed

Residual Risk: Score 2 (Very Low) — Municipality-level aggregation and temporal granularity eliminate most de-anonymization risk; residual risk from sophisticated correlation attack by well-resourced adversary.

Verification: Quarterly de-anonymization risk assessment; annual publication review; monitoring of public data sources.

PR-012: Operator Console Malware

Risk: Operator console compromised via malware on hardened workstation; Score 8 (Medium)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Hardened workstations	Organizational	SEC-9.1	

			Operator workstations configured with baseline security image; unnecessary services disabled; admin access restricted
Endpoint protection (antivirus, EDR)	Technical	OPS-3.2	Endpoint protection software installed and updated; real-time scanning; suspicious process detection
Smart card authentication	Technical	SEC-1.3	Operator console requires smart card + PIN; session cannot be established without hardware token
Session timeout	Technical	SEC-1.4	Operator console sessions timeout after 8 hours of inactivity; automatic logout; re-authentication required
Network isolation	Technical	SEC-4.3	Operator console accessible only from Hätäkeskuslaitos internal network; not internet-exposed; network firewall enforces access
Audit logging of console access	Technical	ARC-6.5	All console access logged with operator identity, timestamp, actions; logs retained for 2 years
User awareness training	Organizational	SEC-1.x	Operator training on phishing, malware, social engineering; annual refresher

Residual Risk: Score 4 (Low) — Hardened workstations and smart card authentication eliminate most malware risk; residual risk from sophisticated spear-phishing or zero-day exploit.

Verification: Quarterly workstation security audit; annual endpoint protection effectiveness assessment; monthly audit log review.

PR-013: SSO Token Theft

Risk: Ministry dashboard compromised via Virtu/Suomi.fi SSO token theft; Score 6 (Medium)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Multi-factor authentication	Technical	SEC-1.3	Virtu/Suomi.fi SSO requires MFA (smart card or mobile authenticator); second factor required for every login
Short token lifetime	Technical	SEC-1.4	SSO tokens expire after 8 hours; refresh tokens expire after 30 days; no long-lived tokens
HTTPS/TLS encryption	Technical	SEC-3.2	All SSO flows use HTTPS with TLS 1.3; certificate pinning for Virtu endpoints

Token validation on every request	Technical	SEC-1.1	Ministry dashboard validates SSO token on every API request; expired or invalid tokens rejected
Read-only scope enforcement	Technical	SEC-2.1	Ministry dashboard API scope is read-only; no state-changing operations possible even with valid token
Session monitoring and anomaly detection	Technical	OPS-1.5	Real-time monitoring of ministry dashboard access; anomalous access patterns (e.g., bulk data export) trigger alerts
Audit logging of dashboard access	Technical	ARC-6.5	All dashboard access logged with actor identity, timestamp, queries; logs retained for 2 years
Quarterly access audit	Organizational	SEC-2.2	Quarterly review of ministry dashboard access logs; verify only authorized officials have access; investigate anomalies

Residual Risk: Score 3 (Low) — MFA and short token lifetime eliminate most token theft risk; residual risk from sophisticated phishing attack or compromised Virtu infrastructure.

Verification: Quarterly access audit; monthly anomaly detection log review; annual SSO flow security assessment.

PR-014: Supply-Chain Attack

Risk: Citizen app compromised via supply-chain attack (e.g., dependency vulnerability); Score 8 (Medium)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Dependency vulnerability scanning	Technical	SDLC-3.2	Automated scanning of all dependencies on every build; known vulnerabilities detected; high-severity findings block build
SBOM generation	Technical	SCS-1.1, SCS-1.2	Software Bill of Materials generated for every release; includes all direct and transitive dependencies; retained for 5 years
Code signing and integrity verification	Technical	SDLC-4.7	App binary signed with Hätäkeskuslaitos certificate; signature verified on installation; tampering detected
App store review process	Organizational	SDLC-2.1	Apple App Store and Google Play review all apps before publication; malicious code detected by store review process
Pinned dependencies	Technical	SDLC-3.2	Critical dependencies (cryptography, JSON parsing)

			pinned to specific versions; no automatic updates; manual review required
Quarterly dependency audit	Organizational	SDLC-3.2	Quarterly review of all dependencies; assessment of maintenance status, security history, alternative options
Incident response plan for compromised dependency	Organizational	OPS-4.1	Plan for rapid response if dependency is compromised; includes app update process, user notification, rollback procedure

Residual Risk: Score 4 (Low) — Dependency scanning and code signing eliminate most supply-chain risk; residual risk from zero-day vulnerability or compromised build system.

Verification: Quarterly dependency audit; monthly SBOM review; annual app store review process assessment.

PR-015: Data Minimization Violation in Phase 2+

Risk: Data minimization principle violated if future phases add unnecessary data collection; Score 9 (Medium-High)

Mitigations:

Mitigation	Control Type	Policy Ref	Implementation
Architecture constraint: no location API in Core API	Technical	ARC-2.2	Core API does not link against location libraries; location must be provided by client app only; prevents unauthorized server-side location collection
Privacy review gate for new features	Organizational	GDPR Art. 25, DATA-7.1	All new features requiring personal data processing must pass privacy review; DPO approval required before implementation
DPIA update process	Organizational	GDPR Art. 35(11)	DPIA reviewed and updated whenever processing activities change materially; Phase 2 features trigger DPIA update
Data minimization principle enforcement	Organizational	GDPR Art. 5(1)(c)	Project charter includes explicit data minimization requirement; feature specifications must justify every data element; unjustified data collection rejected
Code review for data collection	Organizational	SDLC-2.2	All code changes involving personal data require security team review; unnecessary data collection flagged and rejected
Privacy impact assessment for new data	Organizational	GDPR Art. 35	Any new data element requires privacy impact assessment before collection; assessment documented in DPIA
Annual privacy audit			

Organizational	GDPR Art. 5(2)	Annual audit of all personal data collected; verify necessity and proportionality; identify and eliminate unnecessary data

Residual Risk: Score 4 (Low) — Privacy review gate and DPIA update process eliminate most feature-creep risk; residual risk from organizational pressure to collect data for business reasons.

Verification: Privacy review gate for all Phase 2+ features; DPIA update before Phase 2 launch; annual privacy audit.

Control Mapping to Policy Requirements

All mitigations are mapped to specific policy controls to ensure compliance:

Policy	Control	Mitigations
SEC (Security & Access)	SEC-1.x (Authentication)	PR-008, PR-012, PR-013
SEC	SEC-2.x (Access Control)	PR-002, PR-008, PR-013
SEC	SEC-3.x (Data Protection)	PR-002, PR-003, PR-007
SEC	SEC-4.x (Network Security)	PR-001, PR-002, PR-012
SEC	SEC-6.x (API Security)	PR-001
DATA (Data Protection & Privacy)	DATA-2.x (Retention)	PR-007
DATA	DATA-3.x (Privacy)	PR-005, PR-006, PR-009
DATA	DATA-7.x (DPIA)	PR-015
RSK (Risk Management)	RSK-2.x (Risk Assessment)	All mitigations
GDPR	Article 5 (Principles)	All mitigations
GDPR	Article 13 (Privacy Notice)	PR-009
GDPR	Article 15-22 (Data Subject Rights)	PR-005
GDPR	Article 32 (Security)	All technical mitigations
GDPR	Article 35 (DPIA)	PR-015
GDPR	Article 46 (Transfers)	PR-006

Mitigation Verification and Monitoring

Each mitigation includes verification procedures to ensure effectiveness:

Verification Type	Frequency	Owner
Code review	Every pull request	Security team
Security scanning (SAST, DAST, dependency)	Every build	Build automation
Penetration testing	Quarterly	External security firm

Access control audit	Quarterly	Security team
Data retention audit	Quarterly	Database team
Privacy audit	Annual	DPO
Facility security audit	Annual	Facility security
Compliance audit (Katakri, PiTuKri)	Annual	Accredited assessor

Processing Overview

Hälytin is a Finnish national air-threat warning system that processes personal data to deliver real-time alerts from Finnish Defence Forces (FDF) air surveillance to civilian mobile devices. This DPIA covers all personal data processing activities within the Hälytin platform, including device registration, alert delivery, and operational audit logging.

System Purpose

The primary purpose of Hälytin is to provide Finnish residents with immediate notification of inbound air threats, enabling rapid protective action. The system processes personal data to:

1. Receive and register citizen mobile devices for alert delivery
2. Deliver time-critical air-threat notifications to affected populations
3. Maintain audit trails of all operational actions for accountability and post-incident review
4. Enable Sisäministeriö (Ministry of the Interior) and Hätäkeskuslaitos (Emergency Response Centre Agency) to monitor system performance and compliance

Data Subjects

- **Primary data subjects**: Finnish residents (estimated 5.5M population; targeting 3M+ active app installs within 12 months of launch)
- **Secondary data subjects**: Hätäkeskuslaitos operators (estimated 500-1,000 duty officers across regional centres); Sisäministeriö preparedness officials (estimated 20-50)
- **Scope**: All data subjects are located within Finland or physically present in Finland at time of alert dispatch

Data Inventory and Processing Activities

Data Category	Data Elements	Legal Basis	Retention	Recipients	Processing Activities
Device Registration (Citizen)	Device token (hashed), platform (iOS/Android), coarse location (municipality code), language preference, accessibility flags, install timestamp	Vital interests (GDPR Art. 6(1)(d)) for alert delivery; public task (Art. 6(1)(e)) for platform operation	Until device revocation or app uninstall; hashed token retained for 90 days post-revocation to prevent re-registration spam	Core API, Alert Dispatch Service, Device Registry	Registration, token refresh, revocation; delivery targeting; reach metrics aggregation
Device Token (Raw)	FCM or APNs device token in encrypted form	Vital interests (Art. 6(1)(d))	Until device revocation or app uninstall	Core API, Alert Dispatch Service, Secrets Management	Encryption/decryption for push notification dispatch; never logged in plaintext
Coarse Location	Municipality code derived from device registration or cellular location	Vital interests (Art. 6(1)(d)) for geographic alert targeting	Until device revocation or app uninstall	Core API, Alert Dispatch Service, Analytics	Alert targeting; population reach aggregation; no precise GPS retained server-side
Device Metadata	Language preference, ac-			Core API, Alert Dispatch Service	Alert rendering in preferred

	cessibility flags (high contrast, large type, vibration-only mode)	Vital interests (Art. 6(1)(d)) for alert accessibility	Until device revocation or app uninstall		language; accessibility-compliant notification formatting
Install Timestamp	Server-side timestamp of device registration	Vital interests (Art. 6(1)(d)) for aggregate reach metrics	Until device revocation or app uninstall	Core API, Analytics	Aggregate install reach by time period; no per-user temporal tracking
Operator Identity	External identity provider handle (Virtu/Suomi.fi), operator name, role, certification status	Public task (Art. 6(1)(e)) for emergency response operations; legal obligation (Art. 6(1)(c)) for accountability	Long-term (minimum 10 years) for operational accountability	Core API, Audit Service, Hätäkeskuslaitos leadership	Authentication, authorization, audit logging of all operator actions
Operator Actions	Action type (confirm, reject, dispatch, abort, stop-alert), timestamp, incident reference	Public task (Art. 6(1)(e)); legal obligation (Art. 6(1)(c)) for accountability	Minimum 10 years per Finnish record-keeping rules	Audit log, Sisäministeriö, parliamentary oversight on request	Immutable append-only logging; cryptographic chaining
Ministry Official Identity	External identity provider handle (Virtu/Suomi.fi), official name, role	Public task (Art. 6(1)(e)); legal obligation (Art. 6(1)(c))	Long-term (minimum 10 years)	Core API, Audit Service, Sisäministeriö	Authentication, authorization, audit logging of dashboard access
Audit Log Entries	Entity type, entity ID, action, actor ID, actor type, payload (incident details, alert content), timestamp	Public task (Art. 6(1)(e)); legal obligation (Art. 6(1)(c))	Minimum 10 years	Sisäministeriö, Hätäkeskuslaitos, parliamentary oversight	Immutable, cryptographically chained record of all system state changes
Incident Timeline	Threat object details, operator confirmations, dispatch timestamps, delivery counts per channel, all-clear timestamp	Public task (Art. 6(1)(e)); legal obligation (Art. 6(1)(c))	Minimum 10 years	Sisäministeriö, Hätäkeskuslaitos, parliamentary oversight	Post-incident report generation; public accountability; civil-preparedness research
Rejection Events	Rejection reason, operator notification, timestamp	Public task (Art. 6(1)(e))	Minimum 10 years	Audit log, Hätäkeskuslaitos operators	Operator alerting; attack detection (e.g., signature verification failures)
Delivery Receipts	Per-channel delivery confirmation counts, failure counts, timestamp	Public task (Art. 6(1)(e))	Minimum 10 years (as part of incident record)	Audit log, post-incident reports	Alert performance metrics; channel health monitoring

Data Sources

- **Primary source of citizen data**: Citizen Mobile Apps (iOS and Android) during device registration; data provided voluntarily by users
- **Primary source of operator data**: Virtu/Suomi.fi e-Identification infrastructure (external identity provider)
- **Reference data sources**: Maanmittauslaitos (municipality boundaries, public); Tilastokeskus (population statistics, public); FDF Air Surveillance (threat data, classified)

- **Derived data**: Coarse location inferred from device registration or cellular network location; population estimates calculated from public statistics

Data Flows

1. **Device Registration Flow**: Citizen App ’ WAF ’ Core API ’ Device Registry (PostgreSQL) + Cache (Valkey)
2. **Alert Dispatch Flow**: Core API ’ Alert Dispatch Service ’ APNs / FCM / SMS Gateways / Yle / 112 Suomi App
3. **Operator Confirmation Flow**: Operator Console ’ Core API (HTTPS, internal network) ’ Incident Controller ’ Four-Eyes Engine ’ Audit Writer
4. **Ministry Dashboard Flow**: Ministry Dashboard ’ Core API (HTTPS, SSO-gated) ’ Read-only queries
5. **Audit Log Flow**: Core API / Audit Service ’ PostgreSQL (append-only) + Encrypted Object Store (signed exports)

Recipients of Personal Data

Internal recipients (within Hälytin system):

- Core API and Audit Service (all data)
- Alert Dispatch Service (device tokens, coarse location for targeting)
- Device Registry (device tokens, metadata)
- Audit Service (operator identities and actions, ministry official access logs)

External recipients (outside Hälytin system):

- **Apple APNs**: Device tokens (encrypted, transmitted over TLS; Apple does not retain tokens beyond delivery)
- **Google FCM**: Device tokens (encrypted, transmitted over TLS; Google does not retain tokens beyond delivery)
- **Mobile Carriers (DNA, Elisa, Telia)**: Coarse location (municipality-level) for SMS targeting; no device tokens
- **Yleisradio (Yle)**: No personal data; trigger payload only
- **112 Suomi App**: No personal data; alert content only
- **Sisäministeriö**: Aggregate reach metrics (anonymized, municipality-level); incident timelines (operator identities and audit logs); access controlled via SSO and read-only role
- **Hätäkeskuslaitos**: Full audit logs and incident records; access controlled via internal network and role-based authorization
- **Parliamentary oversight**: Full audit logs and incident records on lawful request; access controlled via formal governmental request

Data processors (acting on behalf of Hälytin):

- Finnish sovereign cloud provider (CSC or equivalent PiTuKri-compliant provider) - data hosting, encryption, backup
- HashiCorp Vault or equivalent secrets management system - credential storage and rotation
- Kubernetes infrastructure provider - container orchestration

Cross-Border Data Transfers

Transfers to non-EEA countries:

- Device tokens are transmitted to Apple APNs (USA) and Google FCM (USA) for push notification delivery. These transfers are necessary for the vital-interest purpose (alert delivery) and rely on:
  - **Legal mechanism**: Standard Contractual Clauses (SCCs) with Apple and Google; both companies have committed to data protection frameworks (Apple: APRA/Privacy Shield successor commitments; Google: EU-US Data Privacy Framework)
  - **Supplementary measures**: Device tokens are encrypted in transit (TLS 1.3); raw tokens are not logged or stored by Hälytin in plaintext; tokens are one-way hashed for server-side storage
  - **Transfer Impact Assessment**: Completed; residual risk is low because (a) tokens are pseudonymized (hashed), (b) no precise location is transferred, (c) Apple and Google do not retain tokens beyond delivery, (d) the data subject can revoke at any time by uninstalling the app

No transfers to third countries beyond APNs and FCM. All other processing occurs within Finland (sovereign cloud or on-premises).

Data Retention Schedule

Data Type	Retention Period	Justification	Deletion Method
Device token (raw, encrypted)	Until device revocation or app uninstall	Needed only for active alert delivery	Cryptographic erasure + physical destruction of storage media
Device token (hashed)	90 days post-revocation	Prevent re-registration spam attacks	Automated deletion via background job
Coarse location	Until device revocation or app uninstall	Needed for alert targeting	Cascading delete from database
Device metadata	Until device revocation or app uninstall	Needed for alert rendering	Cascading delete from database
Install timestamp	Until device revocation or app uninstall	Needed for aggregate reach metrics	Cascading delete from database
Operator identity and actions	Minimum 10 years	Legal obligation for governmental accountability; civil-preparedness research	Retention enforced by database policy; deletion requires explicit authorization from Hätäkeskuslaitos leadership
Audit log entries	Minimum 10 years	Legal obligation; regulatory and parliamentary oversight	Immutable append-only; deletion prohibited before retention minimum
Incident timelines	Minimum 10 years	Legal obligation; post-incident review; civil-preparedness research	Retention enforced; deletion prohibited

Data Protection Measures (Summary)

- **Encryption at rest**: AES-256 for all personal data stores (PostgreSQL, Valkey, object storage); customer-controlled keys via Finnish sovereign key management service
- **Encryption in transit**: TLS 1.3 for all external connections; TLS 1.2+ for internal connections; mTLS for service-to-service communication
-

Access control: RBAC enforced at application layer; principle of least privilege (SEC-2.1); role-based authorization for operators and ministry officials

- **Anonymization**: Device tokens stored as one-way hashes; coarse location limited to municipality level; aggregate reach metrics anonymized
- **Audit logging**: Cryptographically chained, immutable audit log; every access and modification recorded
- **Secrets management**: All credentials stored in HashiCorp Vault; rotation enforced; never in source code or logs
- **Network segmentation**: Operator console confined to Hätäkeskuslaitos internal network; public API behind WAF + DDoS protection
- **Vendor security**: All processors (cloud provider, APNs, FCM, carriers) assessed for compliance with DATA policy requirements

Lawful Basis Justification

Vital Interests (GDPR Article 6(1)(d)) is the primary lawful basis for processing citizen device data:

- The processing is necessary to protect the life and physical safety of the data subject (Finnish residents)
- In an air-threat scenario, rapid notification is essential to enable protective action (take shelter, move away from windows, etc.)
- The data subject cannot consent in real-time (alert must be delivered within seconds)
- Vital interests override other legal bases when life safety is at stake
- This is the same legal basis used by emergency response systems in other EU member states (e.g., Ukraine's >a0vB@O=0 B@82>30

Public Task (GDPR Article 6(1)(e)) is the secondary lawful basis for processing operator and audit data:

- Processing is necessary for the performance of a task carried out in the public interest (emergency response and civil protection)
- Hätäkeskuslaitos operates under the Hätäkeskustoiminnasta annettu laki 692/2010 (Act on Emergency Response Centre Operations)
- Sisäministeriö operates under the Pelastuslaki 379/2011 (Rescue Act)
- Processing is authorized by law (Finnish Cybersecurity Act, NIS2 implementation)

Legal Obligation (GDPR Article 6(1)(c)) applies to audit logging and retention:

- Retention of operational records is a legal obligation under Finnish recordkeeping rules and government accountability standards
- Parliamentary oversight of emergency systems requires auditable records

Privacy Notice

Citizens are provided with a privacy notice during app onboarding before any personal data is collected. The notice includes:

- Identity of the controller (Hätäkeskuslaitos on behalf of Sisäministeriö)
- Purpose of processing (delivery of air-threat alerts)

- Lawful basis (vital interests)
- Data categories collected (device token, coarse location, language preference, accessibility flags, install timestamp)
- Recipients (Core API, Alert Dispatch Service, APNs, FCM, SMS carriers)
- Retention period (until revocation/uninstall)
- Data subject rights (access, erasure, portability, restriction, object)
- Right to lodge a complaint with the supervisory authority (Tietosuojavaltuutettu)
- Voluntary nature of participation (users can uninstall at any time)

The privacy notice is provided in Finnish, Swedish, and English, consistent with the alert content languages.