LEGAL DOCUMENT

Privacy and your information

Explains the information used, purposes, recipients and privacy choices.

VERSION	0.6.1
REVISED (UTC)	2026-09-26 01:50:50 UTC
BODY SHA-256	ece67422241717754eb87b4bce7aa2fb2abcefbe6e8d6918882dd2b9c4670d62
PUBLISHED AT	https://www.onsiren.com/legal/privacy/editions/0.6.1

01

Who is responsible

This notice explains the information used by the OnSiren network and Legal Centre, its purposes, access boundaries and your rights.

ONSIREN LIMITED is the entity named in the existing terms. Its company number, address, controller responsibilities and monitored privacy contact must be verified. Existing published information is at https://www.onsiren.com/privacy. The shared network, Legal Centre and private business services require an accurate record of who determines their purposes and essential means. A named privacy lead and the assessment of whether a statutory data protection officer is required remain outstanding.

02

People and information

The service concerns individual security officers, members of the public appearing in alerts, official recipients, business customers and requesters. Account information may include a name, SIA licence information and contact details. Shared alerts may include text, voice, photographs, time and an incident location. Call signs remain personal data when they can be linked to a person.

The Legal Centre receives questions, submitted requests, organisation enquiries and review-workflow applications, authority-verification material and acceptance records. Submitted requests retain the information you provide, their original receipt, status, replies and restricted audit history. Shared information may come from an officer, an authorised organisation or another identified source. Raw verification documents, biometric information and inferred data require separate factual confirmation before they are included in a final notice.

A private browser cookie and server-side session record control access to your request conversations. The record includes a hashed session token, internal browser-owner identifier, role, security token and expiry. Hosted visitor sessions last one hour. An optional recovery code is stored as a hash and can restore access

for 30 days; restoring access ends earlier visitor sessions. Staff use separate account and credential records. These access mechanisms require separate identity checks where a request needs them.

For the public question helper, ordinary question and answer text is processed to provide the on-screen explanation and is not saved in application request or conversation records. The service retains an attempt identifier, hashed browser-owner reference, timestamp and outcome to enforce usage limits. Separate justified retention and disposal schedules for session, recovery, usage, case and audit records remain to be recorded and implemented.

03

Purposes and legal conditions

Each processing purpose must have a recorded legal basis before activation. For a qualifying crime-prevention alert, OnSiren may rely on Article 6(1)(ea), the recognised legitimate interest crime condition, where the specific information, use and audience are necessary. Other safety, account, moderation, intelligence, retention, request and disclosure purposes require their own assessment. Where ordinary legitimate interests under Article 6(1)(f) applies, the purpose, necessity and balancing assessment must be recorded.

Criminal allegations also require Article 10 authority or an applicable DPA 2018 condition. Schedule 1 paragraph 10, as applied by paragraph 36, is a candidate for necessary unlawful-act prevention or detection where seeking consent would prejudice that purpose. Special-category information requires its own Article 9 condition. The final notice must identify the bases and conditions actually adopted; the assessment, appropriate policy document where required and safeguards must support them.

04

Shared alerts and group communication

The agreed design requires the publication screen to identify recipient categories and geographic audience before an officer submits an alert for release. Approved local officers and specifically authorised organisations may receive qualifying alerts within their verified purpose, field, role, place and time limits. Attached voice notes and photographs follow that alert's approved audience.

Ordinary group conversation, its recordings, transcripts and derivatives remain within the group's authorised scope. Official-access permission excludes ordinary private conversation and live officer tracking. The production permissions and publication controls require verification.

05

Identity and location

Call signs and verified eligibility are the ordinary presentation. Real names and SIA details are held separately with restricted access. A request for contact can be relayed to the officer. Disclosure of identity requires its own necessary and lawful decision. Alert location is distinct from a live officer location trail.

Voice, images and context can also identify a person. Accepting a call-sign conversation does not itself authorise release of a name or licence details. The precise location fields, permitted use and exceptional identity-disclosure process remain to be completed.

06

Review and AI

The agreed product design includes AI screening and UK-based human review before release of identifiable third-party alert material. A reviewer must independently assess the report and be able to refuse release, seek information or change the content and audience. AI screening and account verification do not establish that an allegation is true. Detection performance, product enforcement and intended 24/7 moderation coverage require evidence.

The public Legal Centre question helper first matches a question to current published documents within this service. When you explicitly ask a follow-up and OpenAI is configured, the current and previous question and selected published passages are sent to OpenAI for an explanation. The helper uses published material; private cases, restricted research, unpublished edits and live product records are excluded from its retrieval. It has no face-search or autonomous disclosure connection. Answers describe documented positions and do not establish legal verification, complete compliance or an approved individual decision.

Ordinary helper questions do not automatically create a request or enter human triage. The request form has a separate, explicit submission step and returns a tracked receipt. Automatic detection and referral of a rights request typed into the general helper is not implemented. The obligation to identify and handle an actual request received through any available channel remains, as described in clause 10.

AI can support approved routine administration. OnSiren's team administers this workflow and handles escalations. Accountable people remain responsible for consequential decisions. A statutory DPO determination and production accountability assignments remain separate.

07

Retention

The agreed design gives shared alerts a maximum ordinary live display of 24 hours. Its exact start event and stale-report handling remain to be approved. Original alert material and source links have a proposed upper limit of 30 days from original submission, including the live period, with earlier deletion where continued retention is unnecessary and individually justified holds where applicable.

Call-sign histories remain personal data. Long-term statistical outputs need an anonymisation assessment. Account, verification, agreement, privacy-case and security records need separate justified schedules. Each period, backup treatment and deletion process must be verified before it is stated as live behaviour.

08

Recipients, suppliers and transfers

Each approved purpose requires recorded recipients, supplier instructions, locations and safeguards. UK-based moderators do not establish UK-only processing for all systems. A supplier register and transfer assessment remain release dependencies. Neither payment nor a signed agreement alone grants access to identifiable data.

OpenAI processes the current and previous question and selected published passages when you explicitly request an available AI follow-up. A question may contain personal data despite the instruction to keep private case details out of general questions. The server keeps the API key outside the browser and sends no private case records as retrieval context. The OpenAI request uses store:false and enables no tools

or external research. This setting does not establish zero provider retention; applicable provider security, abuse-monitoring and other data-handling arrangements require assessment.

The supplier and recipient notice must identify actual recipients, purposes, processing locations and any restricted overseas transfers, together with the applicable mechanism and how to obtain information about safeguards. OnSiren must verify the provider terms, account settings and actual processing; UK-only processing or completed transfer compliance is not asserted here. Overseas remote access can be relevant. Each transfer requires assessment of the entities and actual processing.

09

Your choices and rights

Anyone can raise access, correction, deletion, restriction, portability or privacy concerns, including officers and non-users. Each right applies according to its legal conditions. Where consent is the basis, you can withdraw it. A reference, approximate date and area can help locate information. A photograph, identity document or account is not a starting requirement; any additional verification must be proportionate.

Your right to object: you can object to processing based on legitimate interests or recognised legitimate interest. The responsible privacy team must assess your circumstances under the applicable rules and explain its decision.

10

Contact and escalation

The public question helper explains published information. To send information into the team's tracked queue, review and submit the Request Centre form; the service then records the request and issues a reference and receipt. You can also use privacy@onsiren.com, the existing published contact whose monitoring must be verified. The form is optional. Requests may arrive verbally or in writing through other available channels and must retain their original receipt date.

The hosted Request Centre accepts public submissions, while product-record search and product-access activation remain unconnected. The general helper does not automatically record or refer questions for human review. If an actual privacy request is received through that helper or another channel, its substance must be assessed, the original receipt preserved and the matter promptly referred to the responsible privacy team without requiring the person to restart the request. Automatic detection and referral from the general helper remains an implementation gap requiring an accountable handling process.

You may also complain to the ICO at https://ico.org.uk/make-a-complaint/. The complaint process must provide acknowledgement, investigation, progress updates and an outcome under the applicable deadlines.

11

People described in someone else's report

OnSiren may receive information about you from a reporting officer or authorised organisation. The applicable notice must explain the source and information categories. Privacy information is supplied within the legal timescale, normally no later than the relevant first disclosure or communication and within one month, subject to a documented exception.

Where individual notification is impossible or would involve disproportionate effort, the responsible team must assess and record that exception and apply safeguards, including publishing the privacy information. Any

crime-prejudice exemption requires its own assessment and applies only to the justified extent. The third-party notice procedure remains a production release dependency.