LEGAL DOCUMENT

# Privacy requests and complaints

Explains privacy requests, complaints and the response workflow.

| | |
|---|---|
| VERSION | 0.6.1 |
| REVISED (UTC) | 2026-09-26 01:50:50 UTC |
| BODY SHA-256 | bd24b4c89aa8d32265a1b789a0ddd53a00136c31dedfd4bead87a990f09d31ac |
| PUBLISHED AT | https://www.onsiren.com/legal/requests/editions/0.6.1 |

This procedure explains how to raise a privacy request or concern and how OnSiren records, assesses and responds to it.

01

## Making a request

Anyone can ask about their information, including security officers, employees and people shown or mentioned in an alert. Requests may arrive verbally or in writing through the Request Centre form, published contact or another available channel. You need no account, special wording or GDPR reference. The original receipt must be recorded and every relevant right or complaint identified. The form remains optional.

The public question helper gives document guidance first and can use OpenAI for an explicit follow-up. Ordinary questions are not saved in application request records or automatically referred for human triage. The separate request form allows the person to review their message, explicitly submit it and receive a tracked reference and receipt. Automatic recognition and referral of an actual rights request typed into the helper is not implemented. If an actual request is received there or through another channel, the responsible team must preserve its original receipt and arrange handling without requiring the person to restart it.

02

## Finding information and verification

A reference, approximate time, place or description can help locate information. A photograph or identity document is not required at first contact. Additional information must be reasonably needed for identification, search or representative authority. Existing verification should be used where sufficient; formal documents are requested only where necessary. Automated facial identification is outside this module.

03

## Timescales

Rights requests are normally answered without undue delay and within one calendar month. Any applicable identity requirement, reasonably necessary SAR clarification pause or permitted extension must be individually assessed, explained and recorded. Staff must validate the right, regime and relevant calendar rules. The system must not silently pause or extend a legal deadline.

Data-protection complaints require acknowledgement within 30 days, appropriate investigation, progress updates and an outcome without undue delay. The acknowledgement period starts the day after receipt; if it ends on a weekend or public holiday, the next working day applies. Tracked privacy questions currently receive a 24-hour internal operational response target. That service target does not replace a statutory deadline. General helper questions enter this queue only through an explicit request submission; an actual rights request received through any channel still requires accountable handling from its original receipt.

04

## Searches, decisions and records

OnSiren must make reasonable and proportionate searches of relevant records, including information held by its suppliers, and explain the outcome. Requested information must not be altered or deleted to prevent disclosure. Targeted preservation requires a justified scope and review date; ordinary lawful retention processes require case-specific handling. A request about information already deleted is answered from the available records.

AI may perform approved routine acknowledgements, triage, organisation and drafted explanations. OnSiren's team administers this review workflow and handles escalated cases. Necessary identity, exemption, disputed-accuracy and sensitive-disclosure decisions must follow the approved human review process. Refusals require reasons and the applicable complaint and court information. Production search, redaction and secure-delivery controls remain unconnected.

05

## Complaints and the Request Centre

A data-protection complaint must be acknowledged, investigated and answered, with progress updates and accessible contact routes. You can raise concerns with the privacy lead and complain to the ICO. A complaint may also contain rights requests requiring linked handling.

The hosted Request Centre accepts public submissions and stores request details, receipts, replies and restricted case history on the service host. A private browser session or recovery code controls requester access; staff administer the queue through restricted accounts. Published portal replies can be read in the request conversation. Outbound email and live product-record search remain unconnected. Include only the information necessary for the request.

Any actual privacy matter received through this service or another available channel retains its original receipt when referred to the responsible team. Automatic rights-request recognition and referral from the general question helper remains unimplemented. The service needs an identified accountable owner, monitored handling arrangements and a justified disposal schedule for the personal data it holds.