LEGAL DOCUMENT

Retention and deletion schedule

Explains separate retention, expiry, deletion and preservation schedules.

VERSION	0.6.0
REVISED (UTC)	2026-09-25 22:03:13 UTC
BODY SHA-256	bc0a0023bdf042b863cf40273a5ac0cc444097b730f327b019be41464229194a
PUBLISHED AT	https://www.onsiren.com/legal/retention/editions/0.6.0

This schedule sets out the intended retention periods, restricted holds and deletion requirements for each information category.

01

Shared safety alerts:

24-hour ordinary recipient visibility. The exact start event for that live clock remains a release decision. Expiry describes the availability of the alert, not resolution of the event.

Reposting, correction or delayed review must not silently give stale material a new live period. A renewed warning needs a current justified purpose and the approved review.

02

Original alert material and source linkage:

working direction of deletion by 30 days from original submission, with documented necessity for any shorter or preserved record. Validate operational purpose, clock, all copies, supplier processing and backups. A lawful hold is narrowly scoped, authorised, reviewable and recorded.

The proposed 30 days includes the live-display period. A hold records the specified records, purpose and authority, access restrictions, owner, review date and release/deletion event. A possible future request does not by itself justify indefinite retention.

03

Long-term intelligence:

retain only outputs that have passed an anonymisation assessment. Remove stable call signs, link keys, images, audio and excessive granular context when needed. Aggregate or suppress rare events. No long-term officer attribution through an alleged anonymous history.

Assess reasonable identification using the output and other available information, including recipient knowledge and rare incidents. Reassess when the data, audience or external information changes. Producing an anonymised output remains a processing operation requiring a basis and safeguards.

04

Accounts and verification:

adopt separate periods tied to eligibility, account service, complaints and legal duties. Raw SIA verification or biometric information requires its own minimisation and supplier review.

Record each category's justified period or criteria, start event, deletion method and responsible owner. Do not retain raw identity or biometric material merely because a supplier makes it available.

05

Agreement, request and security records

Each category requires an approved purpose, access restriction, justified period or clear retention criteria, clock start and disposal method. The Legal Centre host must record a disposal review date and accountable owner before retaining real applicant or requester information. Fixed acceptance evidence and append-only audit design still require a lawful retention architecture. This build contains no real incident archive and makes no claim to have deleted production data.

06

Future union membership and employment casework

Any future union membership or employment casework needs its own notice, purpose, access policy, Article 9 assessment where relevant and retention schedule before collection. Shared-safety alert periods do not govern those separate records. App registration does not itself enrol a person into a union.

07

Evidence:

production deletion jobs need completion records, failed-item queues, hold expiry, backup treatment and restoration tests. Unconnected systems remain marked unknown.

Record failed or incomplete deletion and prevent withdrawn or deleted records returning to ordinary use after restoration. Unconnected controls remain unknown.