LEGAL DOCUMENT

Data sharing and official access agreement

Sets the approved purpose, recipient scope and data-sharing responsibilities.

VERSION	0.6.0
REVISED (UTC)	2026-09-25 22:03:13 UTC
BODY SHA-256	4e646a7d7f7bd0a4e0032ffe872c339375afa94b3019c7efe65f7f6a6493ad41
PUBLISHED AT	https://www.onsiren.com/legal/dsa/editions/0.6.0

01

Parties and purpose

This agreement governs the specific information-sharing purposes and access recorded in the organisation schedule. Execution for live access requires verified legal parties, signatories and a completed schedule. The application directory label identifies the requested organisation; its legal name, statutory or registered identifier, address and signing authority require independent verification. The parties identify each sharing direction, specific safety purpose and necessity in the schedule.

02

Roles, law and responsibility

Each party records its actual controller, joint-controller or processor role for each operation. Each sharing direction identifies the applicable regime, power and lawful basis; additional special-category or criminal-offence conditions and any required policy document; and the DPIA assessment. OnSiren must justify its own disclosure. A competent authority separately assesses whether its law-enforcement purpose falls under Part 3 of the Data Protection Act 2018. Public-body status and this agreement create no general entitlement to information. Required joint-controller arrangements or processor contracts must be completed before those operations begin.

03

Official advisories

Access enables only the functions approved in the schedule. The schedule defines publisher approval, fields and attachments, source permissions, intended local audience, publication and expiry, and correction or recall. Named-person or missing-person notices require verified provenance, necessity and applicable legal conditions. The assessment must address children, offence allegations and sensitive information. A general advisory should use the least identifying information that achieves its purpose.

04

Qualifying shared alerts

The schedule lists the people covered and the exact permitted data fields, attachments, location precision and territory. It also identifies the source, timing, review state and allowed uses. Officer call signs and verified eligibility are the ordinary reporter presentation. Real names and SIA details, routine private chatter, workplace records, shop CCTV and continuous worker location trails are excluded from the ordinary shared feed. Exceptional identity disclosure requires a separate documented lawful and necessary decision. Incident location and call signs may remain personal data.

05

Anonymous intelligence and content rights

Each intended intelligence output requires an identifiability assessment considering linkage, rare events and what recipients may know. Call-sign histories remain personal data. Reassess when sources, detail or recipients change. The parties must also establish source licences, copyright/database rights, confidentiality and permitted commercial use. Existing published commitments concerning personal data and contributed content must be reconciled before commercial reuse. Anonymisation alone cannot determine those separate contractual rights.

06

Recipient and onward-use boundaries

Access is personal to approved organisation personnel for the documented function. Initial BID access covers its own authorised staff; member-business or retailer access requires a separate approved arrangement. The schedule identifies contractors, processor roles and authorised onward recipients. Users must not redistribute, search, profile, train models on or combine information beyond the approved purpose and rights. A required or otherwise lawfully authorised disclosure is assessed, minimised and recorded under its applicable authority. New audiences return to scope review.

07

Accuracy, proportionality and conduct

Recipients treat an allegation as a report requiring assessment and distinguish verified eligibility, human review and independent corroboration. Decisions affecting people must not rely solely on an unverified allegation or AI assessment. Reporting must describe first-hand facts and a specific safety risk. Profiling, intimidation and vigilante uses are prohibited. The schedule names correction/recall owners and contact routes. Where applicable, restrict contested information while verifying accuracy; notify recipients of correction, erasure or restriction unless impossible or disproportionate, and record that assessment. Related exports must be addressed in the recall process.

08

Security, suppliers and personnel

The security annex records verified identity, access controls, appropriate authentication, least privilege, export limits, logging, training, supplier contracts, testing and periodic access review. Reviewer identity access is restricted to the need of the role. UK moderator location is the agreed initial design; the complete provider, hosting, support and access chain requires a separate location and transfer assessment. Each restricted transfer requires the applicable lawful mechanism and assessment. The parties must verify these controls before promising them as implemented.

09

Retention, expiry and holds

The schedule defines periods or criteria and start triggers for each party's display, underlying records, exports, originals, source links, logs and backups. The agreed design provides a 24-hour live alert window and a working limit of 30 days from original submission for routine identifiable originals/source linkage, subject to justification and tested enforcement. Reposting or delayed moderation must not silently renew stale alerts. Recipient evidence retention needs its own lawful purpose. A hold identifies limited records, justification, access, owner, review and release. Ending access triggers the agreed return/deletion process, with any surviving legal duties documented.

10

Rights, complaints and statutory requests

Each party remains accountable for its own obligations and supplies the cooperation and contacts in the schedule. Preserve original receipt dates and forwarding records. Requests may arrive through any valid channel; accessible alternatives must be available. Identify the applicable UK GDPR or Part 3 rules and assess exemptions individually. Communicate required corrections, restrictions and erasures. Public bodies assess FOIA/EIR and other statutory disclosure duties; confidentiality terms do not guarantee an exemption. Complaints need acknowledgement, investigation, updates and an outcome under the applicable rules.

11

Incidents and review

The schedule names breach contacts, escalation routes, available out-of-hours cover, an agreed prompt inter-party reporting target, required initial facts and update arrangements. Each party assesses its own regulator and affected-person notification duties. Record the incident, response and corrective action. Review the arrangement on the agreed date and after material product, law, audience or purpose changes, significant complaints or breaches. A material change requires a revised version and fresh approvals or acceptance where appropriate.

12

Acceptance, commencement and suspension

The complete offer must identify the legal parties, verified signatories, capacities, exact documents and schedule, offer expiry, effective date, duration and execution method. Deliberate acceptance is bound to that package. A notice acknowledgement, contractual acceptance and any data-subject consent are separate concepts. Changed parties, authority or scope require reviewed replacement terms. OnSiren approval and operational activation are separate recorded decisions. Suspension, termination, notice, urgent protective action, review and treatment of retained records must be specified before live execution. The current trial grants no product access.

13

Evidence and copies

Preserve the offered party/authority snapshot, incorporated documents, scope, version, content fingerprint, acceptance statement, authenticated actor and server timestamp. Later lifecycle events retain separate dates. Provide an accessible complete copy that an authorised party can store and reproduce unchanged. A hash supports content integrity; identity and delegation require independent evidence. Evidence records have a justified retention and governed disposal policy, access controls and protected backups.

14

Contractual completion and precedence

Before live execution, complete the parties and contacts; governing law and jurisdiction; execution formalities; effective term; termination and survival; liability and insurance; confidentiality; intellectual property/content rights; service and commercial terms where applicable; dispute routes; and document precedence. These are unresolved business and legal decisions in this trial. No clause approves an unlimited liability allocation or waives statutory rights. The adopted instrument must specify which schedules and service terms govern a conflict.

15

Schedule completion checklist

Each approved schedule must contain: schedule ID and version; legal entities and addresses; named or identified authorised signatories and evidence; per-direction role/regime/power/basis/conditions; purposes and necessity; data-subject categories, exact fields, attachments and source permissions; audience, territory and onward recipients; delivery/search/export limits; review, correction and recall; security and supplier/transfer annexes; retention/hold/disposal rules; rights/FOI and breach contacts; DPIA and security evidence; approval, effective, expiry and review dates; and suspension/termination responsibilities. The present local form captures an initial scope only. The remaining annexes must be completed and verified before production execution.