OSINT Industries LTD
International House, 36-38 Cornhill, London,
England, EC3V 3NG

GENERAL TERMS OF USE AND SERVICE

Website • Free Access • SaaS Platform • API • Training and Professional Services

Effective date: [21/08/2026]

IMPORTANT: Please read these Terms carefully before accessing or using any OSINT Industries website, platform, API, software, training, professional service, content or output. By accessing or using any Service, creating an account, clicking to accept these Terms, or signing an Order that incorporates them, you agree to be bound by these Terms. If you do not agree, you must not access or use the Services.

These Terms are designed primarily for business, governmental, law-enforcement, journalistic, non-profit, compliance, investigative and other professional users. Except for ordinary use of the public Website, the Services are not offered to consumers acting wholly or mainly outside their trade, business, craft or profession unless OSINT Industries expressly agrees otherwise in writing.

1. About us and these Terms:

1.1. OSINT INDUSTRIES LTD is a private limited company incorporated in England and Wales with company number 14974274 and registered office at International House, 36-38 Cornhill, London, England, EC3V 3NG (OSINT Industries, we, us or our).

1.2. These General Terms of Use and Service ("**Terms**") govern access to and use of all products and services that we make available from time to time, including:

a) our public websites, webpages, content, newsletters, downloads and other freely available online resources ("**Website**");

b) free, sponsored, trial, evaluation or promotional access to any hosted application or tool ("**Free Access**");

c) our hosted software-as-a-service applications, investigation platform, dashboards, reports and related features ("**SaaS Services**");

d) our application programming interfaces, software development kits, connectors, developer tools and integration services ("**API Services**");

e) training, workshops, courses, demonstrations, consultancy, implementation, onboarding, configuration and other professional services ("**Professional Services**"); and

f) all documentation, data, content, results, reports, exports, materials, functionality and support supplied with any of the above.

1.3. In these Terms, the Website, Free Access, SaaS Services, API Services, Professional Services and associated materials are together the Services.

1.4. If you access or use the Services for or on behalf of a company, government body, law-enforcement agency, non-profit, partnership or other organisation ("**Organisation**"), you represent and warrant that

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

you have authority to bind that Organisation. In that case, you and your Organisation are jointly referred to as Customer or you.

1.5. If you are an individual accessing only the public Website in a personal capacity, the provisions concerning Orders, fees, subscriptions, API integrations, business indemnities and Professional Services apply only to the extent relevant. Nothing in these Terms excludes any mandatory rights that cannot lawfully be excluded.

2. Key definitions

Term	Meaning
Account	an account created to access any authenticated Service.
API	any application programming interface, endpoint, SDK, token, key, connector or developer service made available by us.
Application	a software application, website, system, product or service developed, operated or controlled by a Customer that connects to an API.
Authorised User	an employee, officer, contractor or other individual whom Customer permits to access a Service for Customer's Permitted Purpose and for whom Customer is responsible.
Biometric Data	personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person that allows or confirms unique identification, including facial biometric templates, embeddings, faceprints and probes and, where used for that purpose, facial images subjected to such processing.
Customer Data	data, search selectors, queries, files, content, instructions, configurations or other material submitted to or transmitted through a Service by or for Customer, including facial images and Biometric Data submitted by Customer or generated solely from Customer-submitted data to execute a Customer-initiated search, but excluding Usage Data.
Documentation	our technical, operational and user documentation, usage instructions, policies and specifications for a Service, as updated from time to time.
Free Service	any Service supplied without charge, including Free Access, free tiers, trials, beta features and public Website content.
Order	an online checkout, order form, quotation, statement of work, subscription confirmation or other ordering document accepted by us that identifies Services, fees, term, usage limits or other commercial terms.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

Term	Meaning
Output	any search result, response, report, visualisation, export, link, profile, indicator, inference, metadata or other information returned or generated through a Service.
Permitted Purpose	Customer's lawful, authorised and ethically appropriate internal business, public-interest, investigative, journalistic, compliance, security, research, governmental, law-enforcement or other professional purpose, as described in an Order, approved during vetting, or otherwise permitted by us in writing.
Subscription Term	the period during which Customer is entitled to access a paid or fixed-term Service.
Third-Party Source	a third-party website, platform, database, public record, API, data provider, open-source project or other external source used by or linked from a Service.
Usage Data	technical, diagnostic, security, billing and service-usage data relating to operation and use of the Services, such as API call counts, feature interactions, latency, errors and account activity, but excluding the substantive content of Customer Data and Outputs except where strictly necessary for security, abuse prevention or support.

3. Contract documents and order of precedence

3.1. The contract between us consists of these Terms, each applicable Order, the Documentation, our Privacy Policy, our Ethics and Compliance Policy, Schedule 1 (Data Processing Addendum), and any service-level agreement or other document expressly incorporated by reference ("**Contract**").

3.2. If there is a conflict, the following order of precedence applies unless an Order expressly states otherwise: (a) a signed Order or statement of work; (b) Schedule 1 (Data Processing Addendum) and any expressly agreed supplemental data-processing terms, solely for personal-data processing matters; (c) a service-level agreement, solely for service levels and remedies; (d) these Terms; and (e) the Documentation and online policies.

3.3. Purchase orders, procurement portals and other Customer documents are administrative only. Any additional or inconsistent terms in them are rejected and do not form part of the Contract unless expressly accepted by us in a document signed by an authorised representative.

4. Eligibility, vetting and authority

4.1. We may require identity, organisation, professional-status, authority, use-case, sanctions, export-control, payment, security or other due-diligence information before or during access to any Service. You must provide complete, accurate and current information and promptly notify us of material changes.

4.2. Access is subject to our vetting and ongoing eligibility assessment. We may refuse, limit, condition, suspend or withdraw access where we reasonably consider that the user, Organisation, jurisdiction, use

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

case or risk profile is unsuitable, unlawful, inconsistent with our Ethics and Compliance Policy, or likely to expose any person or system to harm.

4.3. You must be at least 18 years old and legally capable of entering into the Contract. Authenticated, paid, API and Professional Services are for business or professional use unless we expressly agree otherwise in writing.

5. Accounts, Authorised Users and credentials

5.1. Customer is responsible for all activity under its Accounts, including activity by Authorised Users and any person using Customer credentials, API keys or access tokens, except to the extent caused by our breach of the Contract.

5.2. Customers must ensure that each Account is assigned to a named individual where the Service supports named-user access. Credentials must not be shared, transferred, published or embedded in publicly accessible code or client-side applications.

5.3. Customers must implement reasonable access controls, least-privilege permissions, multi-factor authentication where available, secure credential storage, prompt offboarding, and periodic review of Authorised Users.

5.4. You must notify us immediately at contact@osint.industries if you suspect unauthorised access, credential compromise, security weakness or misuse. We may reset, rotate, revoke or disable credentials where reasonably necessary to protect the Services, users or third parties.

6. Access rights and licences

6.1. Subject to the Contract and during the applicable access period, we grant Customer a limited, non-exclusive, non-transferable, non-sublicensable and revocable right for its Authorised Users to access and use the Services solely for the Permitted Purpose.

6.2. For API Services, Customer may permit its Application and authorised end users to interact with the API only to the extent expressly allowed by the applicable Order and clause 13. Customer remains responsible for all end-user access and use.

6.3. No right is granted by implication. Except for the limited rights expressly stated in the Contract, we and our licensors retain all rights, title and interest in the Services, Documentation, software, models, methods, interfaces, databases, compilation, design, know-how, branding and related intellectual property.

6.4. Free Services are licensed, not sold, and may be withdrawn, restricted or changed at any time. Unless we expressly state otherwise, Free Services do not include support, service levels, data recovery, continuity commitments or any right to future functionality.

7. Public Website and content

7.1. You may view and use the Website and its publicly available content for lawful personal, informational or internal business purposes. You may print or download reasonable extracts for those purposes, provided that proprietary notices are retained and the content is not materially altered or presented misleadingly.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

7.2. You must not use automated tools, crawlers, scrapers, robots, browser automation or similar means to access, copy, index, monitor or extract Website content, except through an API expressly provided for that purpose or with our prior written permission.

7.3. You may link to the Website in a fair and lawful manner that does not damage our reputation or suggest endorsement. You must not frame, mirror or embed the Website or create a link from a website containing unlawful, deceptive, abusive or infringing content.

7.4. Website content is general information only and is not legal, regulatory, financial, investigative or other professional advice. You must obtain appropriate advice and independently verify information before relying on it.

8. Free Access, trials and beta features

8.1. Free Access may be made available to approved users, including government, law-enforcement, journalistic and non-profit users, at our discretion and subject to vetting, usage limits, periodic revalidation and the Permitted Purpose.

8.2. A free trial, promotional period or reduced-price period is governed by the terms displayed or agreed when it begins. It will convert to a paid subscription only where that consequence, the price and the cancellation method are clearly stated and accepted before the trial begins or in an applicable Order.

8.3. Beta, preview, early-access and experimental features may be incomplete, unstable, changed without notice, and withdrawn at any time. They must not be used for production, safety-critical, evidential or legally significant purposes unless we expressly authorise such use in writing.

8.4. We may impose or change usage quotas for a Free Service. Unused searches, credits, calls, seats or other allowances expire at the end of the applicable period and do not roll over unless the relevant Order expressly states otherwise.

9. Orders, subscriptions, fees and payment

9.1. An Order becomes binding when accepted by us, including by email confirmation, activation of the relevant Service, or signature. Access may remain conditional on successful vetting, payment and completion of onboarding requirements.

9.2. Customers must pay the fees stated in the Order. Unless the Order states otherwise: (a) fees are invoiced in advance; (b) invoices are due within 30 days; (c) fees are exclusive of VAT and other applicable taxes; and (d) Customer is responsible for bank, foreign-exchange and payment-processing charges.

9.3. If a customer disputes an invoice in good faith, it must notify us before the due date, identify the disputed amount and reasons, and pay the undisputed portion on time. Overdue undisputed amounts may bear interest at the rate specified in the Order or, if none, 4% per year above the Bank of England base rate, without prejudice to any statutory right to higher interest or recovery costs.

9.4. Fees are non-cancellable and non-refundable except as expressly stated in the Contract or required by law. Expired or unused subscriptions, searches, credits, calls, seats or allowances are not refundable and do not roll over unless an Order says otherwise.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

9.5. A paid subscription renews only as stated in the Order or checkout flow. Where automatic renewal applies, it renews for the period stated in the Order (or, if unstated, a period equal to the expiring Subscription Term) unless either party gives notice of non-renewal at least 14 days before renewal. We may change renewal fees by giving reasonable advance notice, with the new fees taking effect at renewal.

9.6. We may suspend access for overdue undisputed amounts after giving reasonable notice, except where immediate suspension is reasonably necessary to prevent fraud or payment abuse.

10. Lawful, ethical and acceptable use

10.1. Customers must use the Services only for the Permitted Purpose, in accordance with the Contract, Documentation, our Ethics and Compliance Policy, and all applicable laws, regulations, professional duties, court orders, licences, authorisations and codes of practice.

10.2. Before submitting any selector, identifier, personal data or other Customer Data, Customer must have a lawful basis, legitimate authority and proportionate reason to do so. The customer is solely responsible for determining and documenting the legality, necessity, proportionality and fairness of each search, investigation, disclosure and downstream use.

10.3. Where Customer submits Biometric Data or uses facial-recognition, facial-matching or other biometric-identification functionality, Customer must, before each relevant use, identify and document every lawful basis and special-category processing condition required by applicable law, including, where the UK GDPR or EU GDPR applies, an Article 6 lawful basis and a valid Article 9 condition. Where the UK GDPR applies to biometric-recognition functionality, Customer must complete an appropriate data-protection impact assessment before first use and keep it under review; in other jurisdictions Customer must complete any equivalent assessment required by law. Customers must also provide required notices, obtain any required consent or authorisation, and ensure that the search is necessary and proportionate for the Permitted Purpose. Our vetting, activation of functionality or provision of the Service does not constitute a determination or approval of Customer's lawful basis, Article 9 condition, authority or purpose.

10.4. Customers must contextualise and corroborate Outputs, preserve provenance where relevant, apply human judgement, and maintain appropriate records and approvals for sensitive or high-impact uses.

10.5. You must not use or permit use of the Services:

a) for unlawful surveillance, stalking, harassment, intimidation, coercion, blackmail, vigilantism, doxxing, identity theft, impersonation or targeting of individuals without lawful authority;

b) to discriminate unlawfully, persecute protected or vulnerable groups, suppress lawful expression, undermine human rights or the rule of law, or facilitate violence or abuse;

c) to make a solely automated decision that produces legal or similarly significant effects on an individual, unless permitted by applicable law and supported by required safeguards, transparency and human review;

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

d) to determine eligibility for employment, housing, credit, insurance, education, healthcare, immigration or another high-impact service without an independent lawful basis, appropriate verification and any notices, consents or rights required by law;

e) to obtain, infer, expose or exploit highly sensitive information where the use is unlawful, unnecessary, disproportionate or inconsistent with the Permitted Purpose;

f) to investigate a person for a purely personal dispute, curiosity, revenge, romantic, domestic or other non-professional purpose;

g) for spam, bulk marketing, unsolicited contact, credential attacks, phishing, malware, fraud, sanctions evasion, terrorism or other criminal or harmful activity;

h) to access or attempt to access non-public systems, accounts or data without authorisation, or to bypass access controls, rate limits, security measures or technical restrictions;

i) to test the vulnerability of any Service or Third-Party Source without express written authorisation; or

j) in any manner that is likely to cause material harm to a person, interfere with third-party rights, compromise an investigation, contaminate evidence or create a misleading impression of certainty.

10.6. We may require additional approvals, training, use restrictions, audit rights or technical controls for sensitive functionality or use cases, including biometric or facial-recognition functionality. Failure to comply is a material breach.

11. Technical and commercial restrictions

11.1. Except to the extent expressly permitted by the Contract or non-excludable law, Customer must not:

a) copy, modify, adapt, translate, create derivative works from, reverse engineer, decompile, disassemble, discover source code or underlying structure, or test the functioning of any Service;

b) sell, rent, lease, sublicense, distribute, make available, white-label, timeshare or otherwise commercialise the Services or raw Outputs as a standalone product;

c) use the Services or Outputs to create, train, improve, benchmark or validate a competing product, service, database, model or dataset without our prior written consent;

d) bulk-download, harvest, aggregate or build a persistent repository of Outputs beyond what is reasonably necessary for the Permitted Purpose and lawful retention requirements;

e) remove, obscure or alter proprietary notices, source attribution, data-provenance information, warnings or usage restrictions;

f) misrepresent the source, completeness, accuracy, age or meaning of an Output, or state or imply that we, a Third-Party Source or any platform endorses Customer or its conclusions;

g) use the Services in excess of purchased seats, calls, credits, concurrency, volume, geography, use-case or other limits; or

h) interfere with, overload, disrupt or degrade the Services, networks, infrastructure or another user's access.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

11.2. Statutory rights to decompile or observe software may be exercised only to the minimum extent that they cannot lawfully be excluded, after Customer has first requested the necessary information from us and allowed us a reasonable opportunity to provide it.

12. Customer Data, searches and Usage Data

12.1. Customer retains ownership of Customer Data. Customer grants us and our subcontractors a limited, non-exclusive right to host, transmit, process and otherwise use Customer Data only as necessary to provide, secure, support and administer the Services in accordance with the Contract and, where we act as processor, Customer's documented instructions and Schedule 1; to comply with law; and to enforce the Contract.

12.2. Customer represents, warrants and undertakes that it has all rights, permissions, notices, lawful bases, special-category conditions and authority needed for us to process Customer Data in accordance with the Contract, and that Customer Data and its collection, submission, search, matching, use, retention, disclosure and other processing do not infringe any law, duty, confidentiality obligation, privacy right or intellectual-property right.

12.3. Unless an Order or Documentation expressly states otherwise, Customer-submitted facial images and Biometric Data generated solely to execute a biometric or facial-recognition query are processed only for the duration reasonably necessary to execute and return that query and are not used by us for model training, product training, marketing, independent profiling or creation of a general-purpose biometric identity database. We will not retain the substantive facial image or derived biometric template after completion of the query, except to the minimum extent required by applicable law or strictly necessary to investigate a security incident, fraud or prohibited use, in each case subject to appropriate access controls and retention limits.

12.4. We do not acquire ownership of Customer search queries or Outputs. Handling and retention of account information, service interactions, search data and Outputs are described in the Privacy Policy, Documentation, applicable Order and Schedule 1. Customer must not assume that the Services are an evidential archive or backup system.

12.5. We may generate and use Usage Data to operate, secure, monitor, measure, bill, support and improve the Services, detect misuse and produce aggregated or de-identified statistics. We will not use substantive Customer search queries, Customer-submitted facial images, Biometric Data or Outputs to identify Customer's investigative subjects for marketing.

12.6. Customer is responsible for maintaining any copies, case files, audit records, legal holds or evidential materials it requires. Where Customer stores or exports Outputs, Customer must apply lawful retention periods, access controls, data minimisation and secure deletion.

13. Additional terms for APIs and integrations

13.1. Customers may access an API only through credentials issued or approved by us and only in accordance with the Documentation, applicable Order, rate limits, field restrictions, authentication requirements and versioning rules.

13.2. Customer must ensure that each Application:

a) has appropriate security, privacy, authentication, logging, error handling and access controls;
b) provides end users with clear terms and privacy information and obtains all permissions required for data submitted to and received from the API;
c) does not expose API credentials, permit uncontrolled onward access or enable prohibited uses;
d) does not materially alter, omit or obscure provenance, warnings, confidence indicators or restrictions returned with an Output;
e) uses commercially reasonable measures to prevent scraping, credential sharing, excessive calls, abuse and unauthorised extraction; and
f) is operated in compliance with all laws applicable to Customer, its end users and the jurisdictions in which it is made available.

13.3. Customers may store and use API Outputs only to the extent reasonably necessary for the Permitted Purpose, an authorised end-user workflow, evidential integrity or legal retention. Customers must not resell raw API Outputs, create a general-purpose identity database, or allow an end user to query the API outside Customer's controlled Application unless expressly permitted in the Order.

13.4. The customer remains responsible for its Application and end users. Customers must impose terms no less protective of us, the Services, Third-Party Sources, individuals and intellectual property than the relevant provisions of the Contract.

13.5. We may change, deprecate or discontinue an API, endpoint, field or version. Where reasonably practicable, we will give advance notice of a material breaking change to a generally available paid API. We may make immediate changes where required for security, law, third-party source changes or prevention of harm.

13.6. Customers must promptly install or adopt required releases, patches, security updates and supported API versions. We are not liable for issues arising from unsupported versions, Customer modifications, Customer systems or third-party software.

13.7. We may monitor API metadata and usage patterns to verify compliance, protect infrastructure, calculate fees and detect abuse. On reasonable request, Customer must provide information necessary to verify API use and remediate non-compliance. Any audit will be proportionate and subject to reasonable confidentiality safeguards.

13.8. Where an API enables facial recognition, facial matching or other biometric identification, Customer must ensure that each API call is initiated only for a Permitted Purpose and under documented internal authority, is limited to data reasonably necessary for that purpose, and complies with clauses 10, 12 and 18. Customers must not use biometric functionality to create or maintain a general-purpose identity database, persistent watchlist or bulk surveillance capability unless expressly permitted in an Order and demonstrably lawful. We may impose feature-specific vetting, rate limits, audit requirements, technical controls or use restrictions for biometric functionality.

14. Outputs, Third-Party Sources and independent verification

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

14.1. The Services retrieve, organise, link, display or analyse information from Third-Party Sources and public or commercially available sources. We do not control those sources and are not responsible for their availability, legality, accuracy, completeness, security, terms, decisions or continued operation.

14.2. Outputs may be incomplete, unavailable, delayed, duplicated, incorrectly associated, changed or removed by a source, and may reflect aliases, recycled identifiers, historic information or conflicting records. An Output is an investigative lead or data point, not a verified finding, factual determination or statement about a person's character, conduct, identity, guilt or legal status.

14.3. Customers must independently verify and corroborate material Outputs using appropriate sources, methods and human judgement before acting, publishing, disclosing, taking enforcement action or making a decision affecting a person. Customers are responsible for conclusions, reports and actions based on Outputs.

14.4. Links to or references to Third-Party Sources do not imply affiliation, endorsement or approval. Third-party terms, privacy notices, licence conditions and access restrictions may apply, and Customer is responsible for compliance where it directly accesses or uses a Third-Party Source.

14.5. We may add, remove, suspend or change a Third-Party Source or feature at any time, including in response to source changes, legal requirements, ethical review, security concerns or commercial availability.

15. Training and Professional Services

15.1. The scope, deliverables, dates, location, participants, assumptions, dependencies, expenses and fees for Professional Services will be set out in an Order or statement of work. Customers must provide timely access, information, decisions, facilities and suitably skilled personnel reasonably required for delivery.

15.2. Unless an Order states otherwise, training materials are licensed to registered participants for their own internal professional development. They must not be recorded, copied, shared, resold, uploaded to a learning platform, used to train third parties or used to create competing training materials without our prior written consent.

15.3. Professional Services support Customer's own professional judgement. They are not legal advice, authorisation to conduct an investigation, certification of compliance, or a substitute for Customer's policies, approvals, legal advice or operational procedures.

15.4. We may replace instructors or consultants with suitably qualified personnel and may reschedule delivery where reasonably necessary. Cancellation, rescheduling and expense terms in the applicable Order apply. If none are stated, fees for work already performed and non-cancellable commitments remain payable.

15.5. Unless an Order expressly assigns a bespoke deliverable to Customer, we retain ownership of our pre-existing materials, methods, templates, tools, know-how and generic improvements. Upon payment, Customer receives a non-exclusive, perpetual licence to use final deliverables created specifically for Customer for its internal Permitted Purpose.

16. Intellectual property, marks and feedback

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

16.1. All trade marks, logos, service marks and brand elements appearing in or in connection with the Services are owned by or licensed to us. No right to use them is granted without our prior written consent.

16.2. Customers must not register or use any domain name, company name, product name, social handle, keyword or mark that is identical or confusingly similar to our marks, or challenge our ownership or validity of them.

16.3. If Customer provides suggestions, ideas, requests, corrections or other feedback, Customer grants us a worldwide, perpetual, irrevocable, royalty-free right to use and incorporate that feedback without restriction or obligation, provided that we do not identify Customer publicly without consent.

16.4. The Services may include open-source or third-party software subject to separate licence terms. Those terms apply to the relevant components and prevail only to the extent required by the applicable licence.

17. Confidentiality

17.1. Each party receiving confidential Information ("**Recipient**") must keep it confidential, use it only to perform or exercise rights under the Contract, and protect it using at least reasonable care. Confidential Information includes non-public business, financial, technical, security, product, pricing, customer, investigative, operational and strategic information that is marked confidential or should reasonably be understood as confidential.

17.2. Confidential Information does not include information that the Recipient can demonstrate: (a) is or becomes public other than through breach; (b) was lawfully known without restriction before disclosure; (c) is received lawfully from a third party without confidentiality duty; or (d) is independently developed without use of the disclosing party's Confidential Information.

17.3. The Recipient may disclose confidential Information to personnel, professional advisers and subcontractors who need to know it and are bound by confidentiality obligations no less protective than this clause. The Recipient remains responsible for their compliance.

17.4. A Recipient may disclose confidential Information where required by law, court or regulator, but must, to the extent lawful, give prompt notice and reasonable assistance so the disclosing party may seek protective treatment.

17.5. Customer acknowledges that API credentials, non-public Documentation, security information, product roadmaps, technical methods and non-public features are our confidential Information. We acknowledge that non-public Customer Data, investigative workflows and case details are Customer's Confidential Information.

18. Privacy and data protection

18.1. Each party must comply with applicable data-protection and privacy laws in connection with the Contract. Our processing of personal data relating to users, accounts, website visitors and service administration is described in our Privacy Policy.

18.2. For personal data contained in Customer Data that is submitted by or for Customer and processed solely to provide the Services on Customer's documented instructions, Customer acts as controller and we act as processor. This includes, where applicable, facial images, Biometric Data, selectors,

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

identifiers, search instructions, and temporary or intermediate data generated solely to execute a Customer-initiated biometric or facial-recognition search.

18.3. Customer determines and is solely responsible for the purpose, lawful basis, necessity, proportionality and scope of its searches and downstream use. For Biometric Data, customers must identify and document all lawful bases and special-category conditions required by applicable law, including, where applicable, an Article 6 lawful basis and Article 9 condition under the UK GDPR or EU GDPR or any equivalent requirement. Where the UK GDPR applies to biometric-recognition functionality, Customer must complete an appropriate data-protection impact assessment before first use and keep it under review; otherwise Customer must complete any equivalent assessment required by applicable law.

18.4. Where we act as processor, Schedule 1 automatically applies and forms part of the Contract. The applicable Order, Customer's authorised use of the Service and any other written instructions accepted by us constitute Customer's documented instructions only to the extent they are consistent with the Contract and applicable law. We may refuse, suspend or require amendment of an instruction that we reasonably believe would breach applicable data-protection law or the Contract.

18.5. We act as an independent controller for personal data where we determine the purposes and means of processing, including personal data processed for account administration, billing, security, fraud and abuse prevention, legal and regulatory compliance, and Usage Data to the extent it contains personal data. We may also act as an independent controller in respect of data independently obtained, indexed or processed for purposes determined by us. Nothing in the Contract is intended to reclassify the parties' roles where applicable law determines otherwise.

18.6. Customer, as controller, must provide all required notices, obtain any required consents or authorisations, maintain appropriate records of lawful basis and special-category conditions, respond to data-subject requests relating to Customer's purposes and use, conduct required impact assessments, and apply appropriate safeguards to sensitive or high-risk processing. Where we act as processor, we will provide the assistance specified in Schedule 1.

18.7. If the parties are independent controllers for particular processing, each party is separately responsible for its own compliance, transparency, lawful basis, security, retention and response to rights requests.

18.8. Customer must not rely on the public availability of information as, by itself, establishing a lawful basis or unrestricted right to collect, use, disclose, match or retain personal data, including facial images or Biometric Data.

19. Security and service integrity

19.1. We will use reasonable technical and organisational measures designed to protect the Services and personal data against unauthorised access, loss, alteration or disclosure, taking account of the nature of the Services and the risks involved. No system is completely secure, and we do not guarantee that security incidents will never occur.

19.2. Customer is responsible for the security of its devices, networks, Applications, exports, credentials and copies of Outputs, and for configuring the Services appropriately for its use case.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

19.3. Neither party may publicly disclose a vulnerability affecting the other party's systems without first providing sufficient details, allowing a reasonable remediation period, and coordinating disclosure, except where prohibited by law. Testing requires prior written authorisation and compliance with any vulnerability-disclosure policy.

19.4. Customers must cooperate with reasonable investigation and remediation of suspected misuse or security incidents connected with Customer's Account, Application or users.

20. Availability, support and changes to the Services

20.1. We will provide paid generally available Services with reasonable skill and care. Any service levels, support response times, maintenance windows, credits or specific availability commitments apply only if stated in an Order or service-level agreement.

20.2. The Services may be unavailable due to maintenance, updates, emergency work, security events, internet or cloud failures, Third-Party Sources, force majeure, Customer systems or other matters outside our reasonable control.

20.3. We may update, improve, reconfigure or change the Services and Documentation. For paid generally available Services, we will use reasonable efforts not to materially reduce the core functionality purchased during the current Subscription Term, except where required by law, security, ethical review, source availability or prevention of harm.

20.4. Support is provided only to the extent included in the applicable plan or Order. Customers must provide reasonable diagnostic information and cooperate in reproducing and resolving issues.

21. Promises, disclaimers and no sole reliance

21.1. Each party warrants that it has authority to enter into and perform the Contract.

21.2. For a paid generally available Service, we warrant that during the applicable Subscription Term it will perform materially in accordance with the Documentation when used as authorised. Customer's exclusive remedy for breach of this warranty is that we will use reasonable efforts to correct or re-perform the affected Service; if we cannot do so within a reasonable period, Customer may terminate the affected Service and receive a pro-rata refund of prepaid fees for the unused terminated period.

21.3. Free Services, beta features, Third-Party Sources and Outputs are provided "as is" and "as available". To the maximum extent permitted by law, we do not warrant that any Service or Output will be uninterrupted, error-free, complete, accurate, current, secure, compatible with Customer systems, available in every jurisdiction, or suitable for a particular investigation, legal standard, evidential purpose or outcome.

21.4. We do not warrant that an Output identifies a particular person, proves ownership or control of an account, establishes guilt or wrongdoing, or is sufficient for enforcement, publication or a decision affecting an individual. Customers must apply clause 14.

21.5. Except as expressly stated in the Contract and to the maximum extent permitted by law, all conditions, warranties and other terms implied by statute, common law or otherwise are excluded.

22. Customer indemnity

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

22.1. Customer will indemnify us, our affiliates and their officers, employees and contractors against third-party claims, regulatory actions, losses, liabilities, damages, penalties, reasonable legal fees and costs arising from or relating to:

22.2. Customer Data, Customer's Application, or an allegation that either infringes a third party's intellectual-property, privacy, confidentiality or other rights;

a) Customer's or an Authorised User's unlawful, prohibited, negligent or unauthorised use of a Service or Output;

b) Customer's publication, disclosure, retention, decision, enforcement action or other downstream use of an Output;

c) Customer's breach of clause 10, 11, 12, 13, 17, 18 or 19;

d) Customer's collection, submission or use of facial images or Biometric Data, including any failure to establish or document a required lawful basis, special-category condition, investigative authority, notice, consent, impact assessment or other safeguard;

e) an end user, data subject, third party or regulator claim arising from Customer's Application, Customer's search instructions or purpose, Customer's use of biometric or facial-recognition functionality, or Customer's failure to obtain required authority, notices, consents, lawful basis or special-category processing condition.

22.3. We will give Customer prompt notice of an indemnified claim, allow Customer to control the defence and settlement with competent counsel, and provide reasonable cooperation at Customer's cost. Customers may not settle a claim in a way that admits fault by us, imposes an obligation on us or fails to provide an unconditional release without our prior written consent. Failure to notify relieves the customer only to the extent materially prejudiced.

23. Liability

23.1. Nothing in the Contract excludes or limits liability for death or personal injury caused by negligence, fraud or fraudulent misrepresentation, breach of title, or any other liability that cannot lawfully be excluded or limited.

23.2. Subject to clause 23.1, neither party is liable for loss of profit, revenue, business, contracts, anticipated savings, goodwill, reputation, opportunity or data; wasted expenditure; business interruption; or any indirect or consequential loss, in each case arising out of or in connection with the Contract, even if foreseeable or advised of the possibility.

23.3. Subject to clauses 23.1 and 23.4, our total aggregate liability arising out of or in connection with the Contract, whether in contract, tort (including negligence), misrepresentation, restitution, breach of statutory duty or otherwise, will not exceed:

a) for a paid Service, the total fees paid or payable for the affected Service during the 12 months immediately before the event giving rise to the first claim; and

b) for a Free Service or public Website use, £100.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

23.4. Customer's payment obligations and liability under clause 22 are not limited by clause 23.3. Nothing in this clause limits liability to the extent a limitation is unenforceable under applicable law.

23.5. The parties agree that the exclusions and limitations in this clause are reasonable in light of the nature of the Services, Customer's obligation to verify Outputs, the availability of insurance and the allocation of risk reflected in the fees.

24. Suspension and termination

24.1. We may suspend or restrict access immediately where reasonably necessary to address: (a) suspected unlawful or prohibited use; (b) security risk or credential compromise; (c) harm to a person, source, investigation or system; (d) breach of usage limits; (e) overdue undisputed fees; (f) legal, regulatory, sanctions or source requirements; or (g) a material risk to us or another user. Where appropriate, we will notify the customer and allow a reasonable opportunity to remedy.

24.2. Either party may terminate an affected Order or the Contract by written notice if the other party materially breaches it and, where the breach is capable of remedy, fails to remedy it within 14 days after notice. We may terminate immediately for a breach of clauses 4, 10, 11, 13, 17, 18 or 19, or where continued provision would be unlawful or create a serious risk of harm.

24.3. Either party may terminate immediately if the other becomes insolvent, enters administration or liquidation, ceases business, or is subject to an analogous event, except for a solvent restructuring.

24.4. Customers may stop using the Website or a Free Service at any time. We may end a Free Service or Free Access at any time, with or without notice. Paid subscriptions may be terminated for convenience only if and as stated in the applicable Order; termination does not relieve Customer of committed fees.

24.5. We may terminate or refuse renewal where Customer no longer passes vetting, changes its use case without approval, is subject to sanctions or export restrictions, or the relevant Service or Third-Party Source is discontinued.

25. Consequences of expiry or termination

25.1. On expiry or termination, Customer's right to access the affected Services ends and Customer must stop using credentials, APIs, Documentation and other licensed materials. We may disable Accounts and API keys.

25.2. Customers must pay accrued amounts. Unless required by law or an Order, fees already paid are not refundable. If Customer terminates for our uncured material breach under clause 24.2, we will refund prepaid fees for the unused terminated portion of the affected paid Service.

25.3. Customers must delete or return our confidential Information and non-public materials on request, except for archival copies required by law or routine backups not readily accessible, which remain protected.

25.4. Termination does not require Customer to delete lawfully retained Outputs incorporated into case files, reports, legal holds or evidential records, but Customer must continue to comply with applicable law, confidentiality, provenance, security, retention and use restrictions.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

25.5. Clauses intended by their nature to survive will survive, including clauses 11 to 19 and 21 to 29, together with accrued rights and payment obligations.

26. Changes to these Terms

26.1. We may update these Terms and incorporate online policies to reflect changes in law, regulation, security, technology, Services, Third-Party Sources or business practices. We will publish the updated version and effective date and may give notice by email, account notification or another reasonable method.

26.2. For public Website use and Free Services, changes take effect on the stated effective date, and continued use after that date constitutes acceptance.

26.3. For a paid Subscription Term, a materially adverse change will ordinarily take effect at renewal, unless an earlier change is reasonably required by law, regulation, security, ethics, a Third-Party Source or prevention of harm. If such an earlier change materially reduces Customer's contracted rights and Customer objects promptly, the parties will discuss a reasonable solution; if none is available, Customer may terminate the materially affected Service and receive a pro-rata refund of prepaid fees for the unused terminated period.

27. Notices and contact

27.1. Operational notices may be sent by email, through an Account, via the Website or through the Service. Formal legal notices must be in writing and sent by email and, if relating to termination, material breach or a claim, also by tracked post or reputable courier to the relevant registered or notified address.

27.2. Notices to us should be sent to contact@osint.industries and to OSINT INDUSTRIES LTD, International House, 36-38 Cornhill, London, England, EC3V 3NG. Notices to Customer may be sent to the billing, legal, administrative or account contact provided by Customer.

27.3. A notice is deemed received: (a) for email, when sent without a delivery-failure notice, provided that a formal notice sent outside business hours is deemed received at 9:00 a.m. on the next business day in England; and (b) for courier or tracked post, on recorded delivery.

28. General provisions

28.1. Entire agreement. The Contract is the entire agreement concerning its subject matter and supersedes prior proposals, discussions and representations. Each party acknowledges that it has not relied on a statement not set out in the Contract, without limiting liability for fraud.

28.2. Assignment. Customers may not assign, transfer, charge or subcontract its rights or obligations without our prior written consent. We may assign the Contract to an affiliate or in connection with a merger, restructuring or sale of all or substantially all of the relevant business, provided this does not materially reduce Customer's rights.

28.3. Subcontracting. We may use affiliates and subcontractors to provide the Services and remain responsible for their performance to the extent required by the Contract.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

28.4. Force majeure. Neither party is liable for delay or failure caused by events beyond its reasonable control, excluding Customer's payment obligations. The affected party must use reasonable efforts to mitigate the impact.

28.5. No partnership or agency. The Contract does not create a partnership, joint venture, employment, fiduciary or agency relationship. Neither party may bind the other.

28.6. Waiver. A failure or delay to exercise a right is not a waiver. A waiver must be in writing and applies only to the specific circumstance stated.

28.7. Severance. If a provision is invalid or unenforceable, it will be modified to the minimum extent necessary to make it valid and enforceable, or deleted if modification is not possible, without affecting the remaining provisions.

28.8. Third-party rights. A person who is not a party to the Contract has no right to enforce it under the Contracts (Rights of Third Parties) Act 1999, except that our affiliates and indemnified persons may enforce provisions expressly benefiting them. The parties may vary or terminate the Contract without third-party consent.

28.9. Language. The English-language version controls. Translations are for convenience only.

29. Trade controls, anti-bribery and regulatory compliance

29.1. Each party must comply with applicable sanctions, export-control, import-control, anti-bribery, anti-corruption and anti-money-laundering laws in connection with the Contract.

29.2. Customers must not access, export, re-export, transfer or use the Services in or for a prohibited jurisdiction, sanctioned person, restricted end user or prohibited end use. Customers must provide information reasonably requested to verify compliance.

29.3. We may suspend, refuse or terminate access without liability where we reasonably believe provision or use would breach a trade restriction or expose us, our suppliers or a Third-Party Source to sanctions or regulatory risk.

30. Governing law and jurisdiction

30.1. The Contract and any dispute or claim arising out of or in connection with it, its subject matter or formation, including non-contractual disputes or claims, are governed by the laws of England and Wales.

30.2. The courts of England and Wales have exclusive jurisdiction, except that either party may seek urgent interim or injunctive relief in any court of competent jurisdiction to protect confidential information, intellectual property, security or prevent misuse or harm.

30.3. If you are a consumer and mandatory law gives you a right to bring proceedings in another court or provides protections that cannot be excluded, those rights are not affected.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

Schedule 1. Data Processing Addendum

This Schedule 1 applies automatically whenever OSINT Industries processes personal data as a processor on behalf of Customer under the Contract. It is intended to satisfy the requirements applicable to controller-processor arrangements under Article 28 UK GDPR and equivalent data-protection laws. Capitalised terms have the meanings given in the Terms unless this Schedule states otherwise.

1. Scope and roles

1.1. Customer is the controller and OSINT Industries is the processor for personal data described in Annex A to the extent we process that data on Customer's behalf and documented instructions. Customer remains responsible for the lawfulness of those instructions and for compliance with the obligations applying to it as controller.

1.2. If we process personal data for our own independently determined purposes, that processing is outside this Schedule and clause 18.5 of the Terms applies.

2. Documented instructions

2.1. We will process personal data only on Customer's documented instructions, including as necessary to provide the Services described in the Contract, unless applicable UK law requires otherwise. If legally permitted, we will notify the customer before processing required by law.

2.2. We will promptly inform the Customer if, in our reasonable opinion, an instruction infringes applicable data-protection law. We may suspend the affected processing until the parties resolve the issue.

3. Confidentiality and personnel

3.1. We will ensure that persons authorised to process personal data are subject to appropriate confidentiality obligations and receive access only to the extent reasonably necessary for their functions.

4. Security

4.1. We will implement and maintain appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, taking account of the state of the art, implementation costs, the nature, scope, context and purposes of processing, and the risks to individuals.

4.2. Our measures may include, as appropriate, access controls, authentication, encryption in transit and at rest where suitable, logging, vulnerability management, resilience and recovery controls, personnel security, and processes for testing and reviewing security measures.

5. Sub-processors

5.1. Customer gives general written authorisation for us to appoint affiliates and third-party sub-processors necessary to provide the Services. We will maintain or make available a current list of material sub-processors in the Documentation, an applicable Order or another reasonable notice mechanism.

5.2. We will give reasonable notice of an intended addition or replacement of a material sub-processor where required by applicable law. Customers may object on reasonable documented data-protection grounds. The parties will work in good faith to address the objection; if no reasonable alternative is available, we may terminate the affected Service on reasonable notice.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

5.3. We will impose written data-protection obligations on each sub-processor that provide a level of protection materially equivalent to the obligations imposed on us by this Schedule to the extent applicable to the sub-processor's processing. We remain responsible for the sub-processor's performance of those obligations to the extent required by applicable law.

6. Data-subject rights

6.1. Taking account of the nature of the processing, we will provide reasonable assistance through appropriate technical and organisational measures to help customers respond to requests by data subjects to exercise rights under applicable data-protection law.

6.2. If we receive a rights request relating solely to personal data processed for Customer under this Schedule, we may refer the requester to Customer unless law requires us to respond directly.

7. Personal-data breaches

7.1. We will notify Customer without undue delay after becoming aware of a personal-data breach affecting personal data processed under this Schedule and will provide information reasonably available to us that Customer requires to meet applicable notification obligations.

7.2. Our notification or assistance does not constitute an admission of fault or liability.

8. Compliance assistance and impact assessments

8.1. Taking account of the nature of processing and information available to us, we will provide reasonable assistance with Customer's obligations concerning security, breach notifications, data-protection impact assessments and prior consultation with a supervisory authority where required by applicable law.

8.2. The customer remains responsible for determining whether its use of the Services requires a DPIA or regulatory consultation and for the content, conclusions and implementation of those processes.

9. Return and deletion

9.1. On termination or expiry of the relevant Service, and at Customer's choice where reasonably practicable, we will delete or return personal data processed under this Schedule and delete remaining copies, unless applicable law requires retention.

9.2. Notwithstanding clause 9.1, Customer-submitted facial images and derived Biometric Data used solely to execute a facial-recognition or biometric query are subject to the transient-processing and deletion provisions in clause 12.3 and Annex A. Data in routine backups may remain until overwritten in the ordinary course, provided it is protected and not restored except for legitimate disaster-recovery purposes.

10. Information, audits and inspections

10.1. We will make available information reasonably necessary to demonstrate compliance with Article 28 obligations applicable to us as processor. Customers may conduct an audit or appoint an independent auditor, subject to reasonable confidentiality, security and operational safeguards.

10.2. Unless a regulator requires otherwise or there has been a material personal-data breach or credible evidence of material non-compliance, audits will be limited to once in any 12-month period, on reasonable advance notice, during normal business hours, and in a manner that avoids unreasonable disruption. The customer bears its audit costs, and any additional assistance beyond information

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

ordinarily made available may be charged at reasonable rates unless the audit identifies our material breach.

11. International transfers

11.1. We will not make a restricted transfer of personal data processed under this Schedule except in accordance with Customer's documented instructions and a lawful transfer mechanism required by applicable data-protection law, including an adequacy regulation, the UK International Data Transfer Agreement, the UK Addendum to EU Standard Contractual Clauses, or another valid mechanism as applicable.

12. Conflict and survival

12.1. This Schedule prevails over inconsistent provisions of the Terms solely in relation to processing for which we act as processor. The obligations that by their nature should continue after termination survive for so long as we retain relevant personal data.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

Annex A. Processing Details

The following details describe the processing carried out by OSINT Industries as a processor. An Order or Documentation may supplement these details for a particular Service, but may not reduce the protections required by applicable law.

Item	Details
Subject matter	Provision, operation, support and security of the Services used by Customer, including API, investigation and, where enabled, facial-recognition or biometric-search functionality.
Duration	For the applicable Subscription Term or other service period, plus only the limited period required for secure deletion, legal retention or completion of documented post-termination obligations. Facial images and derived biometric templates used solely to execute a query are subject to the shorter transient retention described below.
Nature of processing	Receiving, transmitting, hosting where technically necessary, organising, structuring, retrieving, consulting, analysing, extracting biometric features, creating temporary biometric templates or probes, comparing and matching, returning Outputs, securing, troubleshooting, restricting and deleting personal data.
Purpose	To execute Customer-initiated searches and other documented instructions, provide and secure the contracted Services, and perform support requested by Customer.
Types of personal data	Customer Data containing personal identifiers, selectors, account or profile information, images, facial images, Biometric Data, biometric templates, embeddings, faceprints or probes, search parameters, query metadata, and other personal data contained in Customer submissions or generated solely to execute Customer instructions.
Special-category / sensitive data	Where Customer uses biometric recognition to uniquely identify a person, Biometric Data may constitute special-category personal data. Customer Data may also contain other special-category, sensitive or criminal-offence information depending on Customer's search and use case.
Categories of data subjects	Individuals selected or investigated by Customer; individuals appearing in Customer-submitted images, selectors or records; Customer's Authorised Users; and other individuals whose personal data Customer submits through the Services.
Controller instructions and rights	The customer determines the purpose and scope of each search, may issue lawful documented instructions within the Contract, and retains the rights and responsibilities of the controller under applicable data-protection law.

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization

Item	Details
Facial-recognition retention	Unless an Order or Documentation expressly states otherwise, Customer-submitted facial images and biometric templates or probes generated solely to execute a facial-recognition or biometric query are processed transiently and deleted after completion of the query. They are not retained or reused for model training, product training, marketing, independent profiling or creation of a general-purpose biometric identity database, subject only to the limited legal and security exceptions in clause 12.3.
Other retention	Other Customer Data is retained only for so long as reasonably necessary to provide the Service, comply with documented instructions, meet legal obligations, secure the Service or as otherwise stated in the applicable Order, Documentation or Privacy Policy.
Sub-processors	Affiliates and third-party service providers engaged in accordance with clause 5 of this Schedule and notified through the Documentation, applicable Order or another reasonable notice mechanism.

Schedule 1 above is the Data Processing Addendum incorporated into these Terms; no separate signature is required unless an Order expressly provides otherwise.

Referenced online policies

Privacy Policy: https://www.osint.industries/privacy-policy

Ethics and Compliance Policy: https://www.osint.industries/ethics-and-compliance

Service-specific application matrix

This matrix is explanatory and does not limit the operative provisions above.

Topic	Public Website	Free / Trial	Paid SaaS	API / Integration
Primary access right	View public content	Revocable access within quotas	Subscription right for term	Integration right within Order and Documentation
Vetting	Usually none for browsing	May be required	Required where specified	Generally required
Fees	None	None or promotional	As stated in Order	As stated in Order / usage

Topic	Public Website	Free / Trial	Paid SaaS	API / Integration
Service levels	None	None	Only if expressly agreed	Only if expressly agreed
Output use	Informational only	Permitted Purpose	Permitted Purpose	Controlled Application and Permitted Purpose
Automation	No scraping	Only built-in features	Only built-in features	Only through authorised API
Support	None unless stated	None unless stated	Plan / Order dependent	Plan / Order dependent
Termination	Stop use / content may change	At our discretion	Contract / Order	Contract / Order; keys revoked
Liability cap	£100	£100	12-month affected-service fees	12-month affected-service fees

© OSINT INDUSTRIES LTD., confidential, no transmission without authorization