

Terms and Conditions

Updated: June 2026

IMPORTANT DISCLAIMERS:

WE DO NOT REPRESENT, PROMISE, OR GIVE ANY WARRANTY ABOUT OUR SERVICES OTHER THAN AS SET OUT WITHIN THESE TERMS AND CONDITIONS. IN PARTICULAR, WE DO NOT WARRANT OR REPRESENT THAT: (I) THE SERVICES OR THE CONTENTS OF ANY REPORT, INCLUDING GENERATED OR AI-ASSISTED CONTENT, WILL BE FIT FOR ANY PARTICULAR PURPOSE, OPERATE UNINTERRUPTED OR BE FREE FROM ERRORS, DEFECTS, INACCURACIES, OMISSIONS, FALSE POSITIVES, FALSE NEGATIVES, IDENTITY MISMATCHES OR OUTDATED INFORMATION; OR (II) YOUR USE OF ANY SERVICE OR REPORT WILL RESULT IN COMPLIANCE WITH ANY LAW, RULE, REGULATION, COURT ORDER, PROFESSIONAL DUTY OR REQUIREMENT OF ANY GOVERNMENT OR REGULATORY AUTHORITY.

WE DO NOT WARRANT OR REPRESENT THAT OUR PLATFORM WILL BE FREE FROM VIRUSES, VULNERABILITIES, INTERRUPTION OR DELAY, OR THAT ANY CONTENT ON OUR WEBSITE, PLATFORM, SERVICES OR REPORTS IS ACCURATE, COMPLETE, CURRENT, LAWFUL FOR YOUR PURPOSE OR ADMISSIBLE AS EVIDENCE. OUR SERVICES AND REPORTS DO NOT PROVIDE LEGAL, FINANCIAL, TAX, INVESTMENT, HR, EMPLOYMENT, CREDIT, INSURANCE, TENANCY, SAFEGUARDING, MEDICAL, SECURITY, REGULATORY OR OTHER PROFESSIONAL ADVICE.

FEES FOR EACH ONLINE FIXED-FEE REPORT ARE FEES FOR SIP TO CARRY OUT THE FIXED-FEE RESEARCH AND PREPARE OR MAKE AVAILABLE THE REPORT DESCRIBED ON THE RELEVANT ORDER PAGE. FEES ARE PAYABLE IN ADVANCE AND ARE NON-REFUNDABLE TO THE MAXIMUM EXTENT PERMITTED BY LAW ONCE WE BEGIN WORK, INCUR COSTS, ACCESS PAID SOURCES, PROCESS THE ORDER OR MAKE THE REPORT AVAILABLE. FEES FOR DIRECT INSTRUCTIONS ARE PAYABLE IN ACCORDANCE WITH THE APPLICABLE PROPOSAL, STATEMENT OF WORK, QUOTATION, INVOICE OR WRITTEN CONFIRMATION.

WE DO NOT WARRANT OR REPRESENT THAT OUR SERVICES ARE APPROPRIATE OR AVAILABLE FOR USE IN YOUR COUNTRY OR FOR YOUR INTENDED PURPOSE. THOSE WHO PROCURE OUR SERVICES DO SO ON THEIR OWN INITIATIVE AND AT THEIR OWN RISK. WE MAY REFUSE, SUSPEND, CANCEL OR TERMINATE ANY ORDER OR ACCOUNT WHERE WE BELIEVE THE INSTRUCTION, PURPOSE, METHOD, JURISDICTION, SUBJECT MATTER OR INTENDED USE IS UNLAWFUL, UNSAFE, DISPROPORTIONATE, REPUTATIONALLY HARMFUL OR OUTSIDE SCOPE.

WE SPECIFICALLY DRAW YOUR ATTENTION TO THE REPORT RESTRICTIONS, PROHIBITED USES, DATA PROTECTION OBLIGATIONS, LIMITATION OF LIABILITY AND INDEMNITY PROVISIONS IN THESE TERMS, INCLUDING CLAUSES 11, 12, 16, 21, 22 AND 23.

YOU ARE RESPONSIBLE FOR LAWFUL INSTRUCTIONS TO PROCESS PERSONAL DATA SOLELY FOR THE ACCEPTED PURPOSE OF THE ORDER. YOU REPRESENT AND WARRANT THAT YOU HAVE A VALID LAWFUL BASIS FOR EACH PROCESSING ACTIVITY AND, WHERE SPECIAL-CATEGORY, SENSITIVE, CRIMINAL-OFFENCE, CHILD-RELATED OR OTHER RESTRICTED DATA IS INVOLVED, AN APPLICABLE LEGAL CONDITION UNDER THE RELEVANT LAWS, INCLUDING WHERE APPLICABLE UK/EU GDPR ARTICLES 6, 9 AND 10, UAE DATA PROTECTION LAWS AND OTHER LOCAL DATA PROTECTION LAWS.

YOU ARE RESPONSIBLE FOR PROVIDING ANY REQUIRED NOTICES TO INDIVIDUALS, FOR DETERMINING WHETHER AN EXEMPTION APPLIES, AND FOR YOUR RECEIPT, ACCESS, USE, RETENTION, DISCLOSURE AND DELETION OF ANY REPORT. YOU AGREE TO DEFEND AND HOLD US HARMLESS FROM LOSSES ARISING FROM YOUR UNLAWFUL INSTRUCTIONS, UNLAWFUL PURPOSES, UNLAWFUL USE, UNAUTHORISED DISCLOSURE OR BREACH OF THESE TERMS.

THESE TERMS FORM A BINDING AGREEMENT BETWEEN US

These terms are made up of: (i) the Terms and Conditions set out herein; (ii) the Schedules and Appendices to the Terms and Conditions; (iii) any Order, proposal, statement of work, quotation, invoice or written confirmation that expressly incorporates these terms; (iv) our Privacy Policy; (v) our Cookie Policy; and (vi) any other document or policy referred to within any of the foregoing documents (together, the Agreement).

Our Privacy Policy and Cookie Policy apply to the Platform and Services and should be read together with these Terms.

In the event of any conflict in respect of the provisions of our Agreement and/or the documents referred to in it, the following order of priority shall prevail in descending order of priority, unless mandatory law or mandatory transfer clauses require otherwise:

- (a) any signed written agreement, proposal, statement of work or order confirmation expressly varying these Terms;
- (b) the Schedules contained within these Terms and Conditions;
- (c) the Terms and Conditions;
- (d) our Privacy Policy;
- (e) our Cookie Policy; and
- (f) any other policies or documents referred to herein.

GENERAL TERMS

The following general terms apply to all Customers in all jurisdictions, except to the extent varied by jurisdiction-specific terms or mandatory law.

1. ABOUT US

1.1. SIP International Commercial Information Services LLC operates the website www.SIP-International.com and is registered in the United Arab Emirates under License Number 866821, with an address at The Exchange Tower, Level 19, Business Bay, Dubai, UAE.

1.2. References to SIP International, SIP, we, us or our mean SIP International Commercial Information Services LLC unless an Order, proposal, statement of work or invoice expressly identifies another SIP International group entity as the contracting party for that Order.

1.3. Customers of SIP International group entities, including any UK entity, may access or use the Platform. Unless an Order, proposal, statement of work or invoice expressly identifies another SIP International group entity as the contracting party, the Platform contract is with SIP International Commercial Information Services LLC as the UAE website operator. Where another SIP International group entity is expressly identified as the contracting party for a direct instruction, these Terms apply to that instruction as if references to SIP were references to that entity, unless the relevant proposal states otherwise.

1.4. You can contact us at admin@SIP-International.com.

1.5. SIP does not charge any annual subscription fee unless expressly stated in writing. Charges are based on the specific Services ordered and are displayed at checkout or set out in the relevant proposal, statement of work, invoice or written confirmation.

2. ACCEPTANCE OF THESE TERMS AND CONDITIONS

2.1. By clicking an "I agree" box, registering on the Platform, placing an Order, paying for Services, accessing a Report, using the Platform, downloading a Report, or instructing us directly by email, telephone, messaging service, letter, proposal acceptance or other communication, you agree to be bound by the Agreement.

2.2. If you do not agree to the contents of these Terms and Conditions, do not use our Platform, register for an account, place an Order, pay for Services, access a Report or instruct us to provide any Services.

2.3. Each Order is a separate contract for the relevant Services. A contract is formed when we accept the Order, begin work, issue a proposal or invoice, make a Report available to you, or otherwise confirm acceptance in writing.

2.4. Where you place an Order or instruct us on behalf of a company, employer, public authority, trust, partnership, family office, legal practice, regulated firm or other organisation, you confirm that you have authority to bind that organisation. In that case, the organisation is the Customer and is responsible for the Order, lawful basis, purpose selection, access controls, onward disclosure, retention and use of the Report, and you must disclose the Report only to persons authorised by that organisation and permitted by these Terms.

2.5. The order acknowledgements, customer declarations and purpose confirmations in Schedule 6 form part of the Order process. They may be presented as mandatory unticked checkboxes, radio buttons, declaration boxes, conditional free-text fields or other affirmative confirmations on the Platform before account creation, before submission of an Order and/or before payment for a Fixed-Fee Report. SIP will record the account identifier, Order identifier, date and time, relevant Terms version, selected purpose, recipient/access selection, declarations, payment acknowledgements and other reasonable audit details for

compliance evidence, and you acknowledge and agree that SIP may retain those records in accordance with these Terms and the Privacy Policy.

3. DEFINITIONS AND INTERPRETATION

3.1. In these Terms and Conditions:

'Account Data' means personal data relating to you, your account, your contact details, billing, usage, communications, audit logs and order history.

'Agreement' means these Terms and Conditions, the relevant Order, any proposal, statement of work, quotation, invoice or written confirmation that expressly incorporates them, the Privacy Policy, Cookie Policy and all Schedules.

'Applicable Data Protection Laws' means all data protection, privacy, cybersecurity, electronic communications, direct marketing and data transfer laws that apply to the processing in question, including where applicable the UAE Personal Data Protection Law, the UK GDPR, the Data Protection Act 2018, the EU GDPR, DIFC and ADGM data protection laws, EU Member State data protection laws and equivalent local laws.

'Applicable Laws' means all laws, regulations, regulatory guidance, court orders and binding requirements that apply to a party, an Order, the Services, the Report, Subject Data or your use of the Report.

'Business Customer' means a Customer acting wholly or mainly for business, professional, regulatory, legal, commercial, governmental, charitable or organisational purposes.

'Consumer Customer' means an individual acting wholly or mainly outside their trade, business, craft or profession.

'Customer' means the person or organisation that registers for an account, places an Order, instructs us, pays for Services, receives a Report or uses a Report. You and your refer to the Customer and, where applicable, any authorised user acting on behalf of the Customer.

'Direct Services' means Services ordered directly from us outside the automated online fixed-fee purchase flow, including bespoke OSINT, investigation, surveillance, field enquiries, security services, cybersecurity support, technical surveillance countermeasures, forensic support, asset tracing, fraud support and related services.

'Eligible Purpose' means a lawful, legitimate, specific, proportionate and documented purpose accepted by us for an Order, including one of the purposes described in Schedule 6.

'EU GDPR' means Regulation (EU) 2016/679, as amended or replaced from time to time.

'FCRA' means the United States Fair Credit Reporting Act and related federal or state consumer-reporting laws, rules and regulations.

'Fixed-Fee Report' means an online fixed-fee due diligence, open-source intelligence and public-source research report purchased through the Platform. A Fixed-Fee Report is intended to provide information that may assist the Customer to make its own informed risk assessment decision. It is not a full risk-assessment report and does not constitute legal, financial, tax, employment, credit, insurance, tenancy, safeguarding, AML/KYC compliance, security or other professional advice.

'Order' means each purchase, request, instruction or engagement for Services, whether made through the Platform or directly with us.

'Permitted Recipient' means a person permitted to receive a Report under clause 11.4 or otherwise expressly approved by us in writing.

'Platform' means www.SIP-International.com, any related dashboard, account area, application, API, checkout, payment journey, report delivery system, website functionality and associated systems operated or made available by us.

'Report' means any report, extract, finding, photograph, video, audio, dashboard output, written summary, oral briefing, file, analysis, red flag note or other deliverable produced or supplied by SIP as part of the Services.

'Restricted Data' means personal data that is sensitive, special category, criminal offence, criminal conviction, biometric, health, child-related or otherwise high-risk under Applicable Data Protection Laws.

'Services' means the services provided by SIP, including Fixed-Fee Reports, OSINT research, open-source research, public record searches, database searches, human intelligence, interviews, investigation, surveillance, security services, TSCM, cybersecurity support, forensic support, fraud support, asset tracing, report preparation, analysis, dashboard delivery and related administration.

'Subject' means the person, business, asset, website, account, location or matter that is the subject of an Order or Report.

'Subject Data' means personal data relating to a Subject or to other persons identified in connection with an Order or Report.

'UK GDPR' means the retained EU law version of Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland, as amended or replaced from time to time.

'Working Materials' means source extracts, screenshots, analyst notes, raw search results, operational notes, surveillance logs, drafts and other internal material created or obtained during performance of the Services.

3.2. References to including or includes mean including without limitation. References to laws include those laws as amended, re-enacted, replaced or supplemented from time to time.

4. WE CONTRACT WITH ADULTS AND BUSINESS CUSTOMERS ONLY

4.1. You must be at least 18 years old to use the Platform, register for an account, place an Order, receive a Report or instruct us to provide any Services.

4.2. Our Services are intended for adults and bona fide Business Customers or individuals who have a lawful reason to enter into this Agreement and request our Services.

4.3. Where you are a Business Customer, you represent and warrant that you are acting for legitimate business reasons and have authority to bind, enter into and obligate the business or organisation that you represent.

4.4. If, despite the foregoing, you qualify as a consumer under non-waivable local law, your mandatory rights are preserved. However, these Terms and Conditions are drafted to protect SIP where high-risk reports and investigative services are ordered by individuals or business customers.

4.5. These Terms apply to each Order and to our supply of the Services. They apply to the exclusion of any other terms that you seek to impose or incorporate, or which are implied by law, trade custom, practice or course of dealing, except to the extent mandatory law provides otherwise.

5. OUR OBLIGATIONS

5.1. We will perform the Services with reasonable skill and care.

5.2. Any obligation on us to comply with, or ensure compliance with, any law is limited to laws that are generally applicable to businesses and to providers of similar services. Such obligations do not create an obligation on us to comply with laws or regulations that apply solely to your sector, purpose, professional obligations, regulated activities or intended use unless expressly stated in writing.

5.3. We conduct research, information retrieval, investigation and Report preparation using publicly available or otherwise compliant sources. These may include open-source intelligence, media archives, corporate registries, court index information, land registries, subscription databases, public records, human intelligence, surveillance and similar repositories or resources where accessible and lawful.

5.4. SIP may also provide surveillance teams and other human expertise for matters that may involve fraud, domestic and commercial investigations, digital forensics, forensic accounting, cybersecurity incidents, technical surveillance countermeasures and other relevant investigation or security services.

5.5. Report content and availability vary by jurisdiction and source accessibility. We may decline, suspend, limit or terminate any Order or account where use appears unlawful, unclear, unsafe, disproportionate, unethical, discriminatory, reputationally harmful or outside scope.

5.6. To the extent permitted by law, no warranties, conditions or other terms are implied into this Agreement. We do not warrant or represent that any deliverables or work product will: (i) be fit for any particular purpose; (ii) operate uninterrupted or be free from errors or defects; or (iii) result in your compliance with laws, rules or regulations of any government or regulatory authority.

6. REPORT DISCLAIMER AND SOURCES

6.1. **Informational only; verify before reliance.** Reports compile third-party information that can contain errors, omissions, outdated data, false positives, false negatives, identity mismatches, allegations, context gaps or duplicated information. We do not independently audit all source data and make no guarantees about accuracy, completeness, recency or legal usability.

6.2. **Reports are not legal, financial, tax, employment, HR, credit, insurance, tenant-screening, safeguarding, AML/KYC compliance, regulatory, medical, security or other professional advice.** You should independently verify information and consult qualified advisers as appropriate.

6.3. **Not a consumer report.** Reports are not consumer reports and SIP is not a consumer reporting agency. You must not use any Report for any purpose regulated by the FCRA or similar laws, including employment, promotion, retention, reassignment, tenant screening, credit, insurance, housing, education, licensing, benefits or eligibility determinations.

6.4. Public-domain sourcing. We collect information from open sources reasonably accessible to the public at the time of collection and from other compliant sources. We do not extract data from closed or private social media accounts, bypass access controls, hack systems, install spyware or unlawfully intercept communications.

6.5. Subscriber databases. We may collect information from subscriber, subscription-based or third-party services. Such sourcing is carried out in accordance with applicable laws and source restrictions. We do not guarantee the accuracy, completeness or currency of information provided by any third-party database.

6.6. Human intelligence, surveillance and third-party information. Where an Order requires on-the-ground enquiries, surveillance, interviews or third-party information, our Reports are based on observations and information available at the relevant time. Circumstances may change, persons interviewed may be mistaken or misleading, and surveillance conditions may affect what can be observed.

6.7. Source limitations. We may be unable to reveal the source of information, search terms, operational methods, human sources, contractor identities, database providers or technical methods where disclosure would compromise safety, confidentiality, source protection, legal privilege, contractual restrictions, investigations or security.

6.8. Our Services are to you only. You determine whether, how, when and where to use a Report and bear responsibility for legal compliance of your receipt, access, use, retention, disclosure and deletion of the Report in all relevant jurisdictions.

7. ACCOUNT REGISTRATION

7.1. You agree to provide accurate account information and to keep it updated. You are responsible for all activity occurring under your credentials, except to the extent caused by our breach of these Terms or mandatory law.

7.2. Credential sharing, sublicensing or transfer is prohibited. Each user must have dedicated credentials unless we agree otherwise in writing.

7.3. You must maintain reasonable technical and organisational security for account credentials, Reports, invoices and dashboard content. You must notify us promptly if you suspect unauthorised access, disclosure, loss or misuse.

7.4. We may request identity, authority, purpose, sanctions, payment, anti-fraud, safeguarding or data protection checks before accepting, continuing or delivering any Order.

8. ORDERS AND DIRECT INSTRUCTIONS

8.1. Orders placed through the Platform are subject to acceptance, payment, source availability, jurisdictional limitations and completion of all mandatory acknowledgements and purpose confirmations.

8.2. Direct instructions may be governed by a proposal, quotation, statement of work, invoice, email confirmation or written briefing agreed with us. Unless expressly varied in writing, these Terms apply to all Direct Services.

8.3. You must provide accurate, complete and lawful identifiers, background information and context. This may include names, aliases, dates of birth, jurisdictions, addresses, companies, social media handles, purpose information, authority information and any known risks or restrictions.

8.4. We may decline, suspend, limit, vary or cancel any Order if we reasonably believe that the Order, purpose or intended use is unlawful, unclear, unsafe, disproportionate, unethical, discriminatory, outside our expertise, commercially unsuitable, reputationally harmful or inconsistent with these Terms.

8.5. We do not guarantee that we will accept any Order. Acceptance of one Order does not require us to accept any future Order.

8.6. Delivery times are estimates only unless we expressly agree a binding delivery date in writing. Source availability, jurisdictional limitations, safety constraints, payment checks, legal review, database downtime, third-party delays and operational issues may affect delivery.

9. PRICES; TAXES; PAYMENT; CHARGEBACKS; REFUNDS

9.1. Charges. Fees for online Fixed-Fee Reports are payable in advance at checkout. Fees for Direct Services are as stated in the applicable proposal, quotation, invoice or written agreement.

9.2. Currency. Subject to the nature of the case and applicable jurisdiction, fees may be stated in GBP, USD, AED or another currency. You are responsible for VAT, sales tax, withholding tax, bank charges, exchange charges and other taxes or charges applicable to your Order, except taxes on our own income.

9.3. UAE VAT and other taxes. If UAE VAT or any other tax is chargeable, we may add it to the price at the applicable rate. If a reverse charge, withholding, exemption or zero rating applies, you must provide the information and evidence we reasonably require.

9.4. Payment providers. Online payments may be processed by Stripe or another payment provider. SIP does not store full card numbers, complete payment card details or card security codes. Payment providers may process and retain payment data under their own terms and privacy notices. The dashboard may display limited payment status, invoice and transaction metadata, such as transaction reference or card type/last four digits, where supplied by the payment provider.

9.5. Refunds. Fixed-Fee Report fees are non-refundable once we have begun performance, incurred costs, accessed paid sources, undertaken analysis, processed the Order or made the Report available, except where mandatory law requires otherwise or we agree otherwise in writing.

9.6. Consumer cancellation. If you are a Consumer Customer, you may have statutory cancellation rights under laws that apply to distance contracts, services or digital content. By placing an online Order and ticking the immediate-performance acknowledgement, you request SIP to begin performance immediately and acknowledge that cancellation and refund rights may be limited or lost to the fullest extent permitted by applicable law.

9.7. No outcome-based refunds. Fees are not refundable merely because the Report contains limited information, source data is unavailable, you supplied incomplete or inaccurate identifiers, the Report does not produce the result you hoped for, or jurisdictional, legal, technical or safety limits restrict sources and results.

9.8. Chargebacks. You must not initiate a chargeback without first notifying us and giving us a reasonable opportunity to resolve the issue. We may challenge improper chargebacks and recover our costs where permitted by law.

9.9. Direct instruction invoices. For Direct Services, invoices are payable by the due date stated on the invoice or, if no date is stated, within 14 days of invoice date. Unless otherwise agreed, invoices for Direct Services are payable by bank transfer; where we provide a payment link, payment may instead be made by card through Stripe or another payment provider. We may suspend work for non-payment and recover reasonable collection costs where permitted by law.

10. FIXED-FEE REPORT DELIVERY, DASHBOARD ACCESS AND DELETION

10.1. Fixed-Fee Reports will normally be delivered through your Platform dashboard or by another method we approve. Direct instruction Reports may be delivered by dashboard, secure email, encrypted transfer, oral briefing, written letter or other agreed method.

10.2. Unless the Order page or proposal states otherwise, a Fixed-Fee Report made available on your dashboard must be downloaded promptly. Once first opened or accessed by you, it will be available for 14 days and will then be deleted from, or made inaccessible through, the dashboard without further notice. Backup, audit, legal, tax, dispute, security or compliance copies may be retained outside the customer dashboard only to the extent permitted or required under these Terms, the Privacy Policy or Applicable Laws.

10.3. If a Fixed-Fee Report is not opened within 30 days after upload, we may delete it from the dashboard. We are not required to re-create, re-run or re-deliver a deleted Report unless we agree to do so, and additional fees may apply.

10.4. After dashboard deletion, the dashboard should not retain the Report itself. Your account may continue to show only Account Data, historical order forms, purpose confirmations, invoices, payment status, audit logs and limited order metadata required for tax, accounting, audit, legal, dispute, fraud prevention, security or compliance purposes.

10.5. SIP does not store full payment card numbers, card security codes or equivalent card credentials on the Platform. Card data is handled by Stripe or another payment provider under that provider's own terms and privacy notices.

10.6. Reports will be available through the customer dashboard for 14 days after first access. Unless a longer retention period is required or permitted for legal, regulatory, tax, accounting, audit, dispute, fraud prevention, security, safeguarding, insurance or compliance purposes, SIP will delete or anonymise Report files, Working Materials and Subject Data from its active systems within 60 days after delivery. SIP may retain limited account, order, invoice, payment, acknowledgement, audit and compliance records as described in these Terms and the Privacy Policy.

10.7. Retention periods in the Privacy Policy, DPA, proposal or applicable law may require us to retain some records for longer than the dashboard availability period. This may include invoices, payment records, account records, order forms, purpose confirmations, acknowledgement and declaration records, compliance records, dispute records and legal correspondence. This does not mean SIP agrees to keep a copy of the Report available on the dashboard after the availability period has expired.

10.8. You are responsible for downloading, preserving, securing and lawfully retaining any Report you need after the dashboard availability period. You must not retain a Report for longer than necessary for the accepted Eligible Purpose.

10.9. For clarity, the 14-day dashboard availability period relates to customer access to the Report through the Platform. It does not prevent SIP from deleting or anonymising Reports, Working Materials or Subject Data earlier where lawful and appropriate, or from retaining limited records where required or permitted by law, the Agreement, tax/accounting obligations, legal claims, fraud prevention, security, safeguarding, insurance or compliance requirements.

11. LICENCE TO USE REPORTS

11.1. Subject to payment of all fees and compliance with the Agreement, we grant you a limited, revocable, non-exclusive, non-transferable, non-sublicensable license to download, store and use the Report solely for the accepted Eligible Purpose.

11.2. Reports are branded as SIP International Reports. You must not remove, obscure, replace or alter SIP branding, logos, copyright notices, confidentiality notices, disclaimers, metadata, watermarks or usage restrictions, except with our prior written consent.

11.3. Except as expressly permitted under clause 11.4 or approved by us in writing, you must not resell, republish, distribute, post, upload, make available, lend, share, license, white-label, rebrand, remove or replace SIP branding, include in a third-party database, publish on a blog or website, forward by email, circulate by messaging service, disclose to media, provide to an agent, reseller, investigator or data broker for onward use, add to an AI training dataset, scrape, data-mine, commercially exploit, reproduce in whole or part, or otherwise use a Report outside the license granted in this clause 11.3.

11.4. Permitted Recipients. Subject to applicable law and the accepted Eligible Purpose, you may disclose a Report only to: (i) your own legal advisers, compliance advisers, insurers, auditors or professional advisers who need to know and owe confidentiality obligations; (ii) for Business Customers, internal officers, employees, directors, partners or authorised personnel who need to know and are bound by confidentiality obligations; (iii) a court, tribunal, regulator, law enforcement body or public authority where disclosure is legally required or properly made for the accepted Eligible Purpose; or (iv) any other recipient expressly approved by us in writing.

11.5. Except for disclosure to a Permitted Recipient in accordance with clause 11.4, you must not disclose a Report to the Subject or to any other third party unless you have taken your own legal advice and are satisfied that disclosure is lawful, fair, safe, proportionate and consistent with the accepted Eligible Purpose.

11.6. You must ensure that each Permitted Recipient understands the confidentiality, no-resale, no-publication, data protection and no-misuse restrictions that apply to the Report. You remain responsible for onward disclosure or misuse by Permitted Recipients to the fullest extent permitted by law.

11.7. You must not use any Report to train, fine-tune, test, validate, benchmark or improve any artificial intelligence, machine learning, identity resolution, risk scoring, data broker, search, surveillance, OSINT or competing system.

11.8. You must not create derivative databases, watchlists, risk-scoring systems, searchable repositories, public records, dossiers or commercial intelligence products from Reports.

11.9. All rights not expressly granted to you are reserved by SIP and our licensors.

12. ACCEPTABLE USE

12.1. When using our Platform, Services or Reports, you must not, without limitation:

- breach any laws or regulations, including data protection, privacy, cybercrime, surveillance, confidentiality, harassment, stalking, discrimination, employment, credit, insurance, tenancy, consumer reporting, sanctions or export laws;
- use any Report for any purpose regulated by the FCRA or similar laws, including employment, promotion, retention, reassignment, credit, insurance, housing, tenancy, education, licensing, benefits or eligibility determinations;
- harass, stalk, intimidate, threaten, blackmail, extort, embarrass, defame, dox, shame, exploit, discriminate against or harm any person;
- bypass privacy settings, access closed or private accounts, obtain passwords, hack, intercept communications, install spyware, obtain unlawful location tracking, impersonate another person unlawfully or procure information by deception;
- probe, scan or test vulnerabilities in our Platform without our written consent;
- introduce malware, malicious code, spam, phishing content or harmful material;
- use bots, scrapers, automated tools, fake accounts or shared credentials to access or copy any portion of the Platform or Reports;

- mine, analyse or aggregate our content or data to develop, train, fine-tune, benchmark or validate AI systems or models;
- reproduce, distribute, commercialise or create derivative databases or compilations from our content or any Report data except as expressly permitted;
- use Reports for media, news, gossip, public-facing databases, blogs, social media, influencing, campaigns, political, activist or reputational material without our prior written consent and your own legal review;
- circumvent sanctions, export controls, court orders, platform terms, source restrictions, confidentiality duties or professional obligations; or
- use the Platform, Services or Reports in any manner inconsistent with these Terms.

12.2. If you are unsure whether a proposed use is prohibited, you must not place the Order unless we have first approved the use in writing. Our approval of an Order does not remove your responsibility to ensure your use is lawful.

12.3. We may suspend your account, withhold a Report, delete a Report, refuse future Orders and report relevant matters to authorities where we reasonably suspect prohibited use, unlawful conduct, safeguarding risk, security risk or misuse.

13. CUSTOMER RESPONSIBILITIES

13.1. You will:

- provide accurate identifiers, context, purpose information, authority information and payment information;
- ensure your Order, receipt, use, storage, disclosure and deletion of Reports complies with all Applicable Laws;
- keep account credentials secure and prevent unauthorised access to the Platform, Reports and invoices;
- download Reports promptly within the availability period stated in clause 10 and store them securely only for as long as necessary for the accepted Eligible Purpose;
- limit access to Reports to Permitted Recipients on a strict need-to-know basis and ensure they are bound by appropriate confidentiality and data protection obligations;
- maintain appropriate technical and organisational measures to protect Reports and Subject Data;
- independently verify critical findings and obtain professional advice where appropriate;
- not remove SIP branding, copyright notices, confidentiality notices, watermarks or disclaimers;
- notify us promptly of suspected misuse, unauthorised disclosure, inaccurate identifiers, disputed information, data subject requests, legal claims, regulator contact or security incidents involving a Report; and
- cooperate with reasonable compliance, safety, anti-fraud, data protection, sanctions or misuse checks requested by us.

13.2. You acknowledge and agree that you are solely responsible for ensuring that:

- your intended use of our Services always remains lawful, including in respect of collection, processing, access, storage, disclosure, deletion and use of any personal information;
- any required notices, consents, legitimate interest assessments, data protection impact assessments, transfer assessments and exemptions are obtained or documented;
- you have all lawful bases and meet all other legal requirements under the laws in your jurisdiction and any other relevant jurisdiction to instruct us to process Personal Data and Restricted Data;
- restrictions under UK GDPR, EU GDPR, UAE data protection laws, U.S. federal and state laws, including FCRA, TCPA, CAN-SPAM, GLBA, DPPA and HIPAA, and other international regimes are observed where applicable;
- cross-border transfer safeguards are implemented where required; and
- reasonable retention and secure deletion schedules are applied.

13.3. Where a Report contains information about more than one person, your obligations apply to all personal data in the Report, including information about family members, associates, witnesses, officers, employees, complainants, victims, suspects or other third parties.

14. USE OF AI AND ENRICHMENT

14.1. We may use AI-assisted tools, automated search tools, translation tools, image comparison tools, classification tools, summarisation tools and other technology to help identify, organise, prioritise or present public-source or compliant-source materials.

14.2. AI-assisted outputs may contain hallucinations, artefacts, mismatches, translation errors, outdated material or false positives. We apply reasonable human review appropriate to the Order, but you must independently verify critical findings before relying on them.

14.3. Unless our Privacy Policy or proposal states otherwise, we do not intentionally use Customer-provided Subject Data to train public AI models.

14.4. You must not use Reports as the sole basis for automated decisions or decisions producing legal or similarly significant effects without satisfying all requirements of Applicable Laws.

15. RESTRICTIONS ON SERVICES

15.1. You acknowledge and agree that, when using our Services:

- any mismatches or inaccuracies contained in any Report may arise from inaccurate inputs provided by you or from incomplete, inaccurate or outdated third-party sources;
- we may be unable to reveal the source of any information contained within a Report or provide technical information regarding the techniques or methods we deploy to obtain information;
- we make no warranty that any information contained within a Report is complete, accurate, up-to-date, error-free, legally usable, admissible as evidence or suitable for your intended use;
- you are solely responsible for the lawful use of the information contained within a Report or obtained using our Services, including where it will be used, shared or retained;
- a clean or limited Report does not prove that a Subject is safe, honest, lawful, compliant, low-risk or free from adverse information; and
- an adverse finding may require context, verification, legal analysis or explanation before any reliance.

15.2. Where a Report is intended for legal proceedings, you must instruct legal advisers to consider admissibility, disclosure, privilege, notice, evidence, data protection, confidentiality and procedural requirements before relying on or disclosing the Report.

16. DATA PROTECTION AND PRIVACY; ROLES; SPECIAL/CRIMINAL-OFFENCE DATA

16.1. For more information about our privacy practices, please see our Privacy Policy and Cookie Policy. Those documents explain how SIP processes personal data for account administration, payments, marketing, website analytics, cookies, security, legal compliance and our own business purposes.

16.2. For Subject Data processed to prepare and deliver a Report on your documented instructions, the parties intend that you act as controller and SIP acts as processor or service provider. In practical terms, SIP acts as your data collection, research and report-preparation service provider for that Order; however, the legal role allocation under Applicable Data Protection Laws is controller/processor or controller/service provider unless those laws require a different analysis. If you order as an employee, officer, agent or representative of an organisation, that organisation is intended to be the controller, and you warrant that you have authority to instruct SIP on its behalf.

16.3. You instruct us to process Subject Data only to provide the Services, comply with these Terms, comply with Applicable Laws, protect rights and safety, maintain records permitted by these Terms, and as otherwise documented in the relevant Order.

16.4. You are solely responsible for determining and documenting a valid lawful basis for processing and, where applicable, a valid condition for Restricted Data. You must not instruct us to collect or process data without a valid lawful basis or for any unlawful or prohibited purpose.

16.5. Where UK GDPR or EU GDPR applies, you must identify a lawful basis under Article 6 and, where Restricted Data is involved, a separate condition under Article 9 and/or Article 10 plus any required local law condition before any processing or onward disclosure.

16.6. A legitimate interest or risk-assessment purpose does not automatically make processing lawful. You must assess necessity, proportionality, fairness, transparency, data minimisation, the rights and interests of the Subject, the sensitivity of the data, the likely impact of processing, and whether less intrusive means are available.

16.7. Where UAE data protection law applies, you must ensure that your Order, receipt, use, retention, disclosure and transfer of Subject Data complies with UAE data protection, privacy, cybercrime, surveillance and confidentiality requirements.

16.8. Public-source data may originate from multiple jurisdictions. You consent, acknowledge and agree that we may process and store data on your behalf in the UAE, UK, EEA, United States and other jurisdictions where lawful and necessary for our business operations and Services, and may share data with sub-processors as described in our Privacy Policy or notified to you.

16.9. Schedule 2 forms part of these Terms and applies where SIP processes Subject Data as your processor or service provider. Schedule 3 applies where Subject Data is transferred internationally and transfer terms are required under UK GDPR, EU GDPR or other Applicable Data Protection Laws.

16.10. If a data subject, regulator or authority contacts us about Subject Data processed for your Order, we may forward the request to you, seek your instructions, respond where required by law, or take steps necessary to protect rights, safety, evidence or legal position.

16.11. You are responsible for responding to data subject requests, transparency obligations, notices, lawful basis assessments, DPIAs, transfer assessments, objection handling, deletion requests and challenges relating to your purpose, Order, receipt, use, retention and disclosure of Reports.

16.12. We may refuse or suspend processing where we believe an instruction infringes Applicable Data Protection Laws or would create unacceptable legal, safety, ethical or reputational risk.

16.13. Data Privacy Framework. SIP does not claim certification under the EU-U.S. Data Privacy Framework or its UK Extension and no Data Privacy Framework Program Notice is incorporated into these Terms. Where a restricted transfer requires a transfer safeguard, the parties will rely on the mechanisms described in Schedule 3 or another lawful transfer mechanism, such as the EU SCCs, the UK Addendum, an adequacy mechanism or a statutory derogation.

17. CONFIDENTIALITY

17.1. You and we agree to use each other's confidential information only in relation to the Services and not to disclose it, except where required by law or regulation or to comply with an order of a court or authority of competent jurisdiction.

17.2. Reports, Working Materials, source information, methods, pricing, proposals, credentials, dashboard content, platform information and communications about an Order are SIP confidential information unless we expressly agree otherwise in writing.

17.3. You and we may share each other's confidential information with employees, contractors and professional advisers who have a need to know and are bound by confidentiality obligations.

17.4. Confidentiality obligations do not apply to information that is or becomes public other than through breach, was lawfully known without confidentiality restriction, is independently developed without use of confidential information, or is required to be disclosed by law.

17.5. Upon termination, each party will promptly return or securely destroy the other party's confidential information where required by the Agreement and applicable law, subject to permitted retention for legal, regulatory, tax, accounting, audit, security, safeguarding or dispute purposes.

17.6. You must not publicise your use of SIP, any Report or any findings without our prior written consent.

18. INTELLECTUAL PROPERTY IN OUR SERVICES AND PLATFORM

18.1. SIP and our licensors own all intellectual property rights in the Platform, Reports, report templates, analysis format, database structure, methodologies, logos, branding, trade names, software, code, workflows, searches, tools, know-how and content we provide or create, except for information supplied by you or rights owned by third parties.

18.2. You retain ownership of information you provide to us, but grant us a license to use it to provide the Services, operate the Platform, comply with the Agreement, comply with Applicable Laws, protect rights and safety, maintain appropriate records and exercise our rights.

18.3. No rights are granted except those expressly stated. You must not remove proprietary notices included by us to protect our intellectual property rights.

18.4. We expressly reserve rights and withhold consent to text and data mining of the Platform, Reports or content, including for AI training or evaluation, subject only to exceptions that cannot be excluded by contract under applicable law.

19. SERVICE AVAILABILITY; MODIFICATIONS; SUSPENSION

19.1. Our Platform and Services may be unavailable from time to time due to maintenance, security incidents, third-party outages, source restrictions, internet issues, payment provider issues, legal restrictions or events beyond our control.

19.2. We may modify, discontinue, suspend, throttle, rate-limit or terminate Platform features, Services, accounts or access at any time to protect the Platform, enforce the Agreement, comply with law, prevent misuse, manage sources or address operational requirements.

19.3. We do not guarantee that the Platform will be uninterrupted, error-free, available in all countries, compatible with all devices, free from vulnerabilities or immune from cyber incidents.

19.4. We may suspend or terminate your account, access, Order or Services immediately if we reasonably believe you have breached these Terms, misused a Report, provided inaccurate information, failed to pay, created legal or safety risk, or acted in a way that may harm SIP, a Subject, sources, other customers or third parties.

20. EXPORT CONTROLS AND SANCTIONS

20.1. You represent and warrant that you are not located in, organised under the laws of, or ordinarily resident in any country or territory subject to comprehensive UAE, UK, EU, UN or U.S. embargoes, and that you are not listed on any applicable sanctions list.

20.2. You will not use the Platform, Services or Reports in violation of export controls, sanctions, anti-money laundering, counter-terrorist financing, anti-bribery, anti-corruption or similar laws.

20.3. We may refuse, suspend or cancel any Order or account where sanctions, export controls, anti-money laundering, counter-terrorist financing, anti-bribery, anti-corruption or reputational concerns arise.

21. NO WARRANTIES; DISCLAIMERS

21.1. THE PLATFORM, SERVICES AND REPORTS ARE PROVIDED "AS IS" AND "WITH ALL FAULTS". TO THE MAXIMUM EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. INFORMATION MAY BE INCOMPLETE, OUTDATED, INACCURATE, DISPUTED, MISMATCHED OR UNSUITABLE FOR YOUR INTENDED USE.

21.2. THE EXCLUSIONS OF WARRANTIES AND REPRESENTATIONS SET OUT AT THE HEAD OF THIS AGREEMENT ARE HEREBY REPEATED AND RESTATED IN FULL.

21.3. Nothing in these Terms excludes rights or remedies that cannot be excluded under mandatory consumer, data protection, fraud, personal injury or other applicable laws.

22. LIMITATION OF LIABILITY

22.1. TO THE MAXIMUM EXTENT PERMITTED BY LAW, WE WILL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF PROFITS, REVENUE, DATA, GOODWILL, BUSINESS OPPORTUNITY, ANTICIPATED SAVINGS OR BENEFITS, ARISING FROM OR RELATED TO THE PLATFORM, SERVICES OR REPORTS, EVEN IF ADVISED OF THE POSSIBILITY.

22.2. We will not be liable for loss or corruption of data from your systems, inaccurate source data, identity mismatch, source unavailability, third-party database errors, changes after collection, your unlawful use, your failure to verify findings, your disclosure of Reports, your failure to obtain advice, your failure to provide accurate information, or any decision taken by you or any third party based on a Report.

22.3. Subject to mandatory law, our aggregate liability under this Agreement for claims connected with a Fixed-Fee Report will not exceed the amount you paid for the applicable Fixed-Fee Report giving rise to the claim.

22.4. Subject to mandatory law, our aggregate liability under this Agreement for claims connected with Direct Services will not exceed two times the fees paid or payable for the specific Direct Services giving rise to the claim, or the total fees paid by you to us in the six months preceding the event giving rise to liability, whichever is lower.

22.5. Nothing in this Agreement limits either party's liability for death or personal injury caused by that party's negligence, fraud, fraudulent misrepresentation, wilful misconduct, or anything else that cannot by law be limited.

23. INDEMNIFICATION

23.1. You will defend, indemnify and hold harmless SIP, its affiliates, officers, directors, employees, contractors, agents, suppliers and representatives from and against any third-party claim, loss, liability, fine, penalty, damages, cost and expense, including reasonable legal fees, arising out of or related to:

- your unlawful instructions, unlawful purpose, unlawful use or prohibited use of the Platform, Services or Reports;
- your breach of this Agreement;
- your violation of law or third-party rights, including data protection, privacy, telecoms, confidentiality, harassment, stalking, discrimination, employment, credit, insurance, tenancy, sanctions or consumer reporting laws;

- your receipt, use, retention, disclosure, publication or onward transfer of a Report;
- your failure to have a lawful basis, required condition, notice, consent, exemption, DPIA or transfer safeguard; or
- any claim by a Subject, regulator, authority, employer, counterparty, Permitted Recipient or other third party arising from your Order or use of a Report.

23.2. This indemnity applies to the fullest extent permitted by law and survives termination of the Agreement.

24. IP CLAIMS AND CONTENT COMPLAINTS

24.1. We respect intellectual property rights and expect users to do the same. If you believe that any content or material on our Platform infringes rights you own, please notify us at admin@SIP-International.com.

24.2. Your notice should include sufficient information to identify the relevant material, the rights allegedly infringed, your contact details, evidence of ownership or authority, and the remedy requested.

24.3. Where U.S. law applies, we may respond to notices under the U.S. Digital Millennium Copyright Act or similar procedures. We may remove or disable access to content and terminate repeat infringers in appropriate circumstances.

25. TERM; TERMINATION; EFFECT; SURVIVAL

TERM

25.1. This Agreement applies from the earlier of: (i) your request for our Services; (ii) your use of, or our delivery of, the Services or provision of a Report; (iii) your registration for an account; or (iv) your use of the Platform, and continues unless and until terminated in accordance with these Terms.

TERMINATION

25.2. We may suspend any use of our Platform or Services, remove content, disable any user account, withhold a Report or suspend any Order that we reasonably believe breaches the Agreement or creates legal, safety, security, operational or reputational risk.

25.3. We reserve the right to modify, terminate or otherwise amend fees, features, eligibility criteria, payment methods, sources and service availability associated with the Platform and our Services.

25.4. We may terminate this Agreement or any Order at any time, for any reason, for convenience with or without notice, subject always to our fulfilment of any Services that have been paid for in advance unless we are prohibited by applicable laws or these Terms from doing so.

25.5. You may terminate this Agreement by notifying us in writing or by no longer having a registered account with us, but termination does not entitle you to a refund unless required by mandatory law or expressly agreed by us in writing.

25.6. Either party may terminate immediately for material breach or where the other party enters insolvency, bankruptcy, administration, liquidation, receivership, restructuring or any analogous financial proceedings in any jurisdiction.

25.7. We may terminate immediately without notice if we reasonably believe that continuing the Agreement or any Order may cause us reputational harm, legal risk, safety risk, source compromise or breach of law.

EFFECT OF TERMINATION

25.8. Upon termination, any rights under any license issued under this Agreement are revoked, and you must stop using the Platform and any Report except to the extent continued retention is required by law or for legal claims. You must continue to protect Reports and Subject Data in accordance with these Terms.

25.9. Upon termination, you may no longer be able to access your account or any Reports stored therein or otherwise accessible through the Platform.

SURVIVAL

25.10. Provisions that by their nature should survive termination will survive, including confidentiality, intellectual property, no warranties, disclaimers, Report restrictions, data protection, deletion, limitations of liability, indemnities, governing law and dispute resolution.

26. NOTICES

26.1. Notices to us must be sent by email to admin@SIP-International.com unless we specify another method in writing.

26.2. We may provide notices to you through the Platform, dashboard, email, postal address, registered office, invoice address or other contact details provided within your account or Order.

26.3. If you have a complaint, you should contact us with the Order number, account email, nature of complaint, supporting information and remedy requested. We may require additional information to investigate.

27. CHANGES TO THIS AGREEMENT

27.1. We may update this Agreement from time to time. Material changes may be notified through the Platform or by email and continued use after the effective date constitutes acceptance. If you do not agree, you must stop using the Platform and must not place further Orders.

27.2. Changes do not affect a paid Order already accepted unless required by law, required to protect the Platform or persons, or agreed with you.

28. ASSIGNMENT; ENTIRE AGREEMENT; SEVERABILITY; FORCE MAJEURE

28.1. Assignment and transfer. You may not assign, transfer, novate, charge, subcontract or deal with your rights or obligations under the Agreement without our prior written consent. We may assign or transfer the Agreement to a group company or in connection with a corporate transaction, reorganisation, sale, merger or transfer of business.

28.2. Entire agreement. The Agreement constitutes the entire agreement between you and us concerning the relevant Order and supersedes previous discussions, drafts and communications, except for fraud or fraudulent misrepresentation.

28.3. Severability. If any provision is invalid or unenforceable, it will be modified to the minimum extent necessary to make it valid and enforceable, and the remaining provisions continue in force.

28.4. No waiver. A failure or delay in enforcing any right is not a waiver of that right.

28.5. Force majeure. Excluding your payment obligations, neither party is liable for delays or failures caused by events beyond reasonable control. We will have no liability for delay or failure caused by your breach, third-party acts or omissions not engaged by us, or third-party hardware, software, networks, infrastructure or materials not supplied by us.

28.6. Third-party rights. Except for SIP group companies, officers, directors, employees, contractors, agents, suppliers and representatives who may enforce clauses intended to protect them, no person other than the parties has rights to enforce the Agreement unless mandatory law provides otherwise.

28.7. Language. These Terms are drafted in English. Any translation is for convenience only. The English version prevails to the extent permitted by law.

29. GOVERNING LAW AND DISPUTE RESOLUTION

29.1. Subject to clause 29.4, clause 29.5, Schedule 3 and mandatory law, these Terms, each Order and any non-contractual obligations arising out of or in connection with them are governed by the laws of England and Wales.

29.2. Subject to clause 29.4, clause 29.5, Schedule 3 and mandatory law, the courts of England and Wales have exclusive jurisdiction to resolve any dispute arising out of or in connection with these Terms, any Order, the Services, Reports or any non-contractual obligations arising out of or in connection with them.

29.3. For Business Customers and Direct Services only, a proposal, statement of work or signed written agreement may state that disputes will instead be finally resolved by arbitration seated in London, conducted in English by one arbitrator under the rules specified in that proposal, statement of work or agreement. Either party may seek urgent interim, injunctive, confidentiality, intellectual property, data protection, misuse, security or preservation relief in any court with jurisdiction.

29.4. If you are a Consumer Customer, mandatory consumer laws in your country of residence may give you rights to bring or defend claims in local courts or under local law. Nothing in this clause deprives you of those mandatory rights.

29.5. Either party may seek urgent interim, injunctive, confidentiality, intellectual property, data protection, misuse, security or preservation relief in any court with jurisdiction.

SCHEDULE 1 - JURISDICTIONAL SPECIFIC TERMS

1. UNITED ARAB EMIRATES

1.1. SIP International Commercial Information Services LLC is established in the UAE. UAE Federal Decree-Law No. 45 of 2021 concerning the Protection of Personal Data and other UAE privacy, cybercrime, surveillance, confidentiality, evidence, licensing, sanctions and public order laws may apply depending on the Services, data, location, Customer, Subject and intended use.

1.2. You must not instruct us to obtain, process, access, use, disclose or retain information in a manner that breaches UAE law. You are responsible for your own compliance with UAE law where you are established in the UAE, use Reports in the UAE, target a UAE Subject or transfer data to or from the UAE.

2. UNITED KINGDOM AND EUROPEAN UNION

2.1. The terms of the DPA within Schedule 2 apply to our processing of Subject Data for UK and EEA Customers where UK GDPR or EU GDPR applies.

2.2. To the extent UK GDPR or EU GDPR applies, you are the controller and SIP is your processor for Report preparation, unless Applicable Data Protection Laws require a different role allocation. You must ensure a valid lawful basis under Article 6 and, where applicable, valid conditions for special-category data under Article 9 and criminal-offence data under Article 10 plus local law before any processing or onward disclosure.

2.3. The terms of Schedule 3 apply to restricted transfers from the UK or EEA to SIP in the UAE or another third country where transfer safeguards are required.

2.4. For UK/EU Customers, we expressly reserve the right and withhold consent to text and data mining of the Platform, Reports or content, including for AI training or evaluation, subject only to exceptions that cannot be excluded by contract under Directive (EU) 2019/790 and equivalent UK provisions.

3. UNITED STATES

3.1. We are not a U.S. company, not a consumer reporting agency and not a provider of consumer reports. Reports must not be used for any purpose regulated by the FCRA or similar U.S. federal or state laws, including employment, promotion, retention, reassignment, credit, insurance, housing, tenant screening, education, licensing, benefits or eligibility determinations.

3.2. You must not use the Services or Reports in a manner that violates GLBA, DPPA, HIPAA, COPPA, CAN-SPAM, TCPA, state privacy laws, stalking, harassment, doxxing, protected-person address confidentiality laws, or analogous U.S. federal or state laws.

3.3. If a Report relates to a U.S. person or will be used in the United States, you are solely responsible for obtaining U.S. legal advice before ordering, using, disclosing or retaining it.

4. REST OF THE WORLD

4.1. You are responsible for compliance with local laws in your country of establishment, in places where Reports are used, and in jurisdictions where data was sourced or where the Subject is located. We do not represent that the Services are appropriate or available in all jurisdictions.

4.2. Except where prohibited by mandatory law, the governing law and dispute resolution provisions in clause 29 apply to Customers outside the UAE, UK, EEA and United States.

SCHEDULE 2 - DATA PROCESSING ADDENDUM

This Data Processing Addendum (DPA) sets out the terms and conditions upon which you appoint us to act as your processor or service provider and governs our processing of Subject Data that is required to provide the Services under this Agreement.

1. ROLES AND SCOPE

1.1. The Customer is controller of Subject Data and SIP is processor or service provider when SIP processes Subject Data to prepare and deliver a Report on the Customer's documented instructions, unless Applicable Data Protection Laws require a different role allocation.

1.2. SIP is controller of Account Data and personal data processed for SIP business administration, billing, fraud prevention, compliance, security, legal claims, personnel, contractor management, source management, tax, accounting and statutory obligations.

1.3. If Applicable Data Protection Laws characterise either party differently for any processing activity, the parties will cooperate in good faith to comply with the applicable role allocation. This DPA will be interpreted to give effect to mandatory data protection requirements.

2. CUSTOMER INSTRUCTIONS

2.1. The Customer instructs SIP to process Subject Data for the following purposes: receiving and assessing Orders, carrying out lawful OSINT and investigation tasks, collecting public-source and compliant-source information, analysing and verifying information, preparing Reports, delivering Reports, administering Orders, handling support, compliance, security, legal claims, source integrity, deletion and related purposes.

2.2. The Agreement, Order, purpose selection, proposal, written communications and any lawful written instruction from the Customer comprise the Customer's documented instructions.

2.3. SIP must promptly inform the Customer if, in SIP's opinion, an instruction infringes Applicable Data Protection Laws, unless prohibited by law from doing so.

3. CUSTOMER OBLIGATIONS

3.1. The Customer represents and warrants that it has all lawful bases, notices, consents, exemptions, legitimate interest assessments, sensitive data conditions, criminal offence data conditions, DPIAs, transfer safeguards and other authorisations required to instruct SIP to process Subject Data.

3.2. The Customer is responsible for purpose limitation, data minimisation, lawfulness, fairness, transparency, data subject rights, accuracy checks after receipt, retention decisions, onward disclosure, security, deletion and use of Reports.

3.3. The Customer must not instruct SIP to process Subject Data for any unlawful, prohibited, discriminatory, unfair, excessive or unsafe purpose.

4. SIP PROCESSOR OBLIGATIONS

4.1. SIP will:

- process Subject Data only on documented instructions, unless required by Applicable Laws;
- ensure personnel and contractors authorised to process Subject Data are subject to confidentiality obligations;
- implement appropriate technical and organisational measures taking account of the nature, scope, context and purposes of processing and the risks to individuals;
- assist the Customer, taking account of the nature of processing and information available to SIP, with data subject rights, DPIAs, security, breach notifications and regulator consultations where required by Applicable Data Protection Laws;
- notify the Customer without undue delay after becoming aware of a personal data breach affecting Subject Data processed as processor, and in any event within 48 hours where reasonably practicable;
- maintain records required by Applicable Data Protection Laws;
- delete or return Subject Data after the end of Services in accordance with clause 10 and this DPA, unless retention is required or permitted by Applicable Laws or the Agreement; and
- make available information reasonably necessary to demonstrate compliance with this DPA, subject to confidentiality, security, privilege, source protection and proportionality requirements.

5. SUB-PROCESSORS

5.1. The Customer gives SIP general authorisation to appoint sub-processors and service providers required to provide the Services, including hosting providers, cloud infrastructure providers, payment providers, communications providers, database providers, analytics providers, security providers, contractors, investigators and professional advisers.

5.2. SIP will impose written terms on sub-processors that provide a level of protection for Subject Data materially equivalent to this DPA, taking account of the nature of the services.

5.3. SIP remains responsible to the Customer for sub-processor processing of Subject Data to the extent required by Applicable Data Protection Laws, subject to the liability limitations in the Agreement.

5.4. SIP may publish or provide a list of material sub-processors in the Privacy Policy or on request. The Customer may object to a new sub-processor on reasonable data protection grounds, but acknowledges that refusal may prevent SIP from providing the Services.

6. SUBJECT MATTER, DURATION, NATURE AND PURPOSE

6.1. Subject matter: processing Subject Data for OSINT reports, investigations, surveillance, security services, analysis, reporting, dashboard delivery, direct instructions and related administration.

6.2. Duration: from Order assessment until deletion or anonymisation of Subject Data in accordance with clause 10, this DPA, the Privacy Policy, the Order and Applicable Laws.

6.3. Nature of processing: collection, recording, organisation, structuring, storage, retrieval, consultation, analysis, enrichment, verification, matching, compilation, disclosure to the Customer, restriction, deletion, anonymisation and related operations.

6.4. Purpose: to provide the Services requested by the Customer and to comply with the Agreement and Applicable Laws.

7. CATEGORIES OF DATA SUBJECTS AND PERSONAL DATA

7.1. Data subjects may include Subjects, alleged aliases, family members, associates, employees, officers, directors, shareholders, beneficial owners, counterparties, witnesses, complainants, victims, suspects, litigation parties, public figures, public officials and other persons identified in connection with an Order or Report.

7.2. Personal data may include names, aliases, photographs, videos, audio, contact details, addresses, dates of birth, nationality, occupation, education, employment, companies, directorships, assets, property, financial information, litigation, adverse media, social media content, public records, online identifiers, location information, relationships, opinions and contextual information.

7.3. Restricted Data may include information revealing or suggesting criminal allegations, criminal convictions, offences, proceedings, political opinions, religion, ethnicity, health, disability, sex life, sexual orientation, biometric information, child-related information or other sensitive matters where relevant and lawful.

8. SECURITY MEASURES

8.1. SIP will maintain technical and organisational measures appropriate to the risk, which may include access controls, least-privilege access, confidentiality obligations, secure systems, reasonable encryption or secure transmission, account authentication, segregation of customer matters where appropriate, logging, monitoring, misuse controls, secure deletion or anonymisation, incident response, supplier due diligence and personnel instructions.

8.2. The Customer acknowledges that no system, platform, email, database, communication channel or transfer method is guaranteed to be completely secure.

9. DELETION AND RETURN

9.1. Subject to the Agreement and Applicable Laws, Fixed-Fee Reports will be deleted from the dashboard in accordance with clause 10. Working Materials may be deleted or anonymised within 60 days after delivery unless longer retention is required or permitted.

9.2. At the Customer's written request, SIP will delete or return Subject Data processed as processor, unless retention is required or permitted by Applicable Laws, legal claims, audit, tax, insurance, safeguarding, security, source protection or the Agreement.

9.3. SIP may retain limited records to evidence the Order, purpose, instructions, compliance, invoice, payment, delivery, deletion, dispute handling, misuse investigation and legal position.

10. AUDIT AND ASSISTANCE

10.1. SIP will provide reasonable information necessary to demonstrate compliance with this DPA. Any audit must be reasonable, proportionate, subject to confidentiality, limited to information relevant to the Customer's Subject Data and conducted in a manner that does not compromise security, source protection, other customers, privilege or operations.

10.2. On-site audits are not permitted unless required by Applicable Data Protection Laws or agreed in writing. The Customer must pay SIP's reasonable costs of assistance, audit support and information requests unless the request arises from SIP's material breach of this DPA.

SCHEDULE 3 - INTERNATIONAL DATA TRANSFER TERMS

This schedule is intended to address restricted transfers from the UK, EEA or another jurisdiction with transfer restrictions to SIP in the UAE or another third country.

1. RESTRICTED TRANSFERS FROM THE UK OR EEA TO SIP

1.1. Where the Customer is established in the UK, EEA or another jurisdiction with transfer restrictions and transfers Subject Data to SIP in the UAE or another third country as processor, the Customer is the data exporter and SIP is the data importer, unless the applicable transfer law requires a different analysis.

1.2. For EEA restricted transfers, the EU Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 apply as follows: Module 2 (controller to processor); Clause 7 docking clause applies; Clause 9 general written authorisation for sub-processors applies; Clause 11 optional language is not used; Clause 17 governing law is the law of the EU Member State in which the exporter is established or, where unavailable, Irish law; and Clause 18 jurisdiction is the courts of the relevant EU Member State or, where unavailable, Ireland.

1.3. For UK restricted transfers, the UK International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner applies to the EU SCCs described above, with the tables completed by the information in this Schedule.

1.4. If the UK, EU or another relevant authority replaces, amends or approves alternative transfer clauses or mechanisms, the parties agree that the updated mechanism will apply to the extent required by Applicable Data Protection Laws.

2. SCC/UK ADDENDUM TABLE DETAILS

Topic	Details
Exporter	The Customer identified in the relevant Order, account, proposal, statement of work, invoice or written confirmation.
Importer	SIP International Commercial Information Services LLC, License Number 866821, The Exchange Tower, Level 19, Business Bay, Dubai, UAE, or the SIP group entity identified in the relevant Order.
Exporter role	Controller, unless the Order states otherwise.
Importer role	Processor or service provider for Subject Data processed to provide the Services.
Activities	Processing Subject Data to provide OSINT, investigation, surveillance, security, analysis, reporting, dashboard delivery, direct instructions and related administration.
Categories of data subjects	As described in Schedule 2, paragraph 7.1.
Categories of personal data	As described in Schedule 2, paragraph 7.2.
Restricted Data	As described in Schedule 2, paragraph 7.3, where relevant, lawful, necessary and proportionate.
Frequency	One-off or continuous, depending on the Order and account relationship.
Retention	As described in clause 10, Schedule 2 and the Privacy Policy.
Sub-processors	General authorisation as described in Schedule 2, paragraph 5. A list may be provided in the Privacy Policy or on request.
Security measures	As described in Schedule 2, paragraph 8 and any applicable security documentation.
Competent supervisory authority	For EEA transfers, the supervisory authority determined under Clause 13 of the EU SCCs. For UK transfers, the Information Commissioner.

3. TRANSFER ASSESSMENTS AND SUPPLEMENTARY MEASURES

3.1. The Customer is responsible for determining whether a restricted transfer occurs and for completing any required transfer risk assessment, data transfer impact assessment or equivalent assessment. SIP will provide reasonably available information to assist where required by Applicable Data Protection Laws.

3.2. The Customer acknowledges that SIP may process and store data in the UAE and may use sub-processors in the UAE, UK, EEA, United States and other jurisdictions as described in the Privacy Policy, sub-processor list or Order.

3.3. The parties will implement supplementary measures where required and reasonable, taking account of the nature of the data, purpose of the transfer, available technology, source restrictions, security requirements, costs and risks.

3.4. SIP is not certified under the Data Privacy Framework and does not rely on it as a transfer mechanism unless SIP expressly states otherwise in writing. Where a U.S. sub-processor is certified under the Data Privacy Framework and the transfer is eligible, SIP may rely on that certification together with any additional safeguards required by Applicable Data Protection Laws; otherwise, the transfer will rely on another appropriate transfer safeguard where required.

SCHEDULE 4 - MINORS AND SAFEGUARDING EXEMPTION

1.1. SIP does not accept online Fixed-Fee Report Orders where the Subject is under 18 or is believed to be under 18.

1.2. SIP will not knowingly provide Services involving a child under 13 except where required by law, law enforcement, a court, a regulator, a safeguarding authority or another exceptional circumstance approved by SIP in writing and supported by specialist legal review.

1.3. For Subjects aged 13 to 17, SIP may consider a direct instruction only where: (i) the purpose is a genuine safeguarding, welfare, legal claim, missing person, fraud prevention or protective purpose; (ii) the Customer has legal authority; (iii) processing is necessary and proportionate; (iv) the Customer has documented the lawful basis and any required conditions; and (v) SIP approves the instruction in writing before work begins.

1.4. The Customer must provide evidence of authority, age band, safeguarding purpose, lawful basis, sensitive data condition, notices or exemptions, DPIA or risk assessment, and any relevant court, school, authority or legal documentation requested by SIP.

1.5. SIP will not use unlawful methods, contact a child, bypass private accounts, procure access credentials, encourage deception, or process illegal child sexual abuse material. If illegal material is encountered, SIP may preserve minimal necessary information and report to appropriate authorities as required by law.

1.6. SIP may refuse or stop any child-related or safeguarding instruction at any time where SIP believes the instruction is unsafe, unlawful, disproportionate, abusive, retaliatory, connected with harassment or domestic abuse, or otherwise inappropriate.

SCHEDULE 5 - DIRECT INVESTIGATION, SURVEILLANCE AND SECURITY SERVICES TERMS

1.1. This schedule applies to direct instructions for investigation, surveillance, human intelligence, security, TSCM, cybersecurity support, forensic support, asset tracing, fraud support, matrimonial or domestic investigations and related services.

1.2. Direct Services will be subject to agreed scope, location, time, method, deliverables, risk assessment, personnel availability, safety requirements, legal restrictions, budgets and expenses.

1.3. The Customer must provide accurate background, purpose, authority, legal context, known risks, court orders, restraining orders, domestic abuse concerns, weapons concerns, safeguarding concerns, mental health concerns, police involvement, access restrictions, property rights and any other information relevant to safety and lawfulness.

1.4. SIP will not knowingly carry out or facilitate unlawful trespass, unlawful interception, hacking, unlawful access to devices or accounts, unlawful tracking, unlawful recording, bribery, impersonation, entrapment, intimidation, harassment, stalking, deception prohibited by law, or any other unlawful method.

1.5. Surveillance and human intelligence are inherently uncertain. Weather, visibility, traffic, source availability, subject behaviour, police activity, access, health and safety, local law, property rights and operational constraints may affect results.

1.6. Reports from Direct Services are based on observations and information available at the relevant time. Circumstances may change. Third-party statements may be inaccurate, incomplete or deliberately misleading. You must verify critical findings and obtain legal advice before reliance.

1.7. Operational methods, routes, equipment, personnel identities, source identities, risk assessments, database providers and security measures are confidential and may be withheld where disclosure would compromise safety, source protection, legal privilege, contractual restrictions, investigations or security.

1.8. The Customer is responsible for obtaining legal advice on use of evidence, admissibility, disclosure, privilege, service, court orders, regulatory reporting, employment action, termination, confrontation, safeguarding, policing and any other action based on Direct Services.

1.9. SIP may suspend or terminate Direct Services immediately where there is safety risk, suspected unlawful purpose, suspected domestic abuse misuse, stalking risk, child risk, source compromise, police involvement, refusal to provide required information, non-payment or reputational risk.

1.10. Unless expressly agreed in writing, fees for Direct Services exclude travel, accommodation, database charges, specialist equipment, translation, local counsel, court attendance, witness statements, notarisation, legalisation, expert reports, emergency work and expenses, which may be charged separately.

SCHEDULE 6 - WEBSITE REGISTRATION AND CUSTOMER ACKNOWLEDGEMENTS

1. Status and presentation

1.1. This Schedule sets out the account registration details, acknowledgements, declarations, purpose confirmations, recipient and access selections and payment confirmations that form part of the Order process under clause 2.5.

1.2. The Platform is not required to present this Schedule as a single document during registration or checkout. The relevant wording, or a combined declaration to the same effect, may be presented at the appropriate stage of the registration, order and payment journey, including as mandatory unticked checkboxes, radio buttons, declaration boxes, single-selection fields or conditional information fields.

1.3. Confirmations given on the Platform in that manner have the same legal effect as if given in the form set out in this Schedule, and SIP may record and retain them as described in clause 2.5.

2. Account registration

2.1. To create an account, you must provide accurate and complete registration details, including your full name, email address and, where requested, your mobile number, and you must keep those details up to date.

2.2. You must state whether you are registering as an individual or on behalf of an organisation, employer, client or other principal. If you register as an individual, you must provide your residential address and country of residence. If you act for an organisation or other principal, you must provide your role or title, the name and address of the organisation or principal, its country of establishment and confirmation of your authority to act on its behalf.

2.3. Your account credentials are personal to you. You must keep them secure and must not share them or permit any other person to use your account unless SIP agrees otherwise in writing.

3. Account acknowledgements

3.1. When you register, you will be asked to confirm, whether individually or by a combined declaration, that:

- (a) you are at least 18 years old;
- (b) the account information you have provided is accurate and complete and you will keep it up to date;
- (c) you are registering for your own lawful use, or you are authorised to register on behalf of the organisation, employer, client or other principal you represent;
- (d) if you register or place an Order on behalf of an organisation, employer, client or other principal, you have authority to bind that person or organisation and to provide instructions to SIP on its behalf;
- (e) neither you, nor any organisation or principal you represent, is subject to applicable sanctions or owned or controlled by a sanctioned person, and you will not use the Platform, Services or Reports in breach of sanctions, export control, anti-money laundering or counter-terrorist financing laws;
- (f) you understand that SIP provides online fixed-fee due diligence, open-source intelligence and public-source research reports and may separately provide Direct Services by written proposal or written agreement;
- (g) you understand that Reports and Services may involve personal data, including sensitive, special-category, criminal-offence, child-related or other restricted data;
- (h) you will only order and use Reports for a lawful, legitimate, specific, proportionate and documented purpose;
- (i) you have read and agree to these Terms and Conditions, including the Report restrictions, prohibited uses, data protection obligations, liability limits and indemnities; and
- (j) you have read SIP's Privacy Policy and Cookie Policy.

4. Order details for Fixed-Fee Reports

- 4.1.** Before submitting an Order for a Fixed-Fee Report, you must review and, where necessary, update your account details and confirm whether the Order is placed as an individual or on behalf of an organisation, employer, client or other principal.
- 4.2.** You must provide the Subject identifiers relevant to the Order, which may include name, aliases, date of birth or age range if known, company names, social media handles, email addresses, phone numbers, websites, addresses, jurisdictions and any other identifiers relevant to the Order. Accurate identifiers reduce the risk of identity mismatch.
- 4.3.** Where known, you should provide the countries, locations or connections relevant to the Subject. If these are not known, you may state “unknown” and provide the information available to you. SIP may request further details or decline the Order where sanctions, safety or legal risk arises.
- 4.4.** You must confirm for each Order that you do not know or suspect that the Subject is under 18. If the Subject is, or may be, under 18, you must not place an Order online and must contact SIP at client@sip-international.com for written approval before placing any Order (see paragraph 10 of this Schedule and Schedule 4).
- 4.5.** For each Order you must select who will receive or access the Report (paragraph 5) and the purpose of the Order (paragraph 6).

5. Recipients and access

- 5.1.** You must select who will receive or access the Report from the following categories:
- (a) you only;
 - (b) authorised personnel within the organisation, employer, client or other principal you represent who need to know and are bound by confidentiality obligations, where you are a Business Customer and access is necessary for the accepted Eligible Purpose;
 - (c) legal advisers, compliance advisers, insurers, auditors or other professional advisers who need to know and owe confidentiality obligations, where disclosure is lawful, necessary and consistent with the accepted Eligible Purpose;
 - (d) a court, tribunal, regulator, law enforcement body or public authority, where disclosure is legally required or properly made for the accepted Eligible Purpose; or
 - (e) another recipient, in which case you must provide details of that recipient, and SIP's approval is required before the Order is accepted or before the Report is disclosed to that recipient.

6. Purpose of the Order

- 6.1.** You must select the main purpose that applies to each Order from the following:
- (a) legal claims or proceedings: the Report is required for potential, threatened, current or contemplated civil or criminal legal proceedings, legal claims, asset recovery, enforcement, fraud investigation, dispute resolution, litigation support or obtaining legal advice;
 - (b) personal or business risk assessment: the Report is required before entering into, continuing or exiting a personal, family, investment, commercial or business relationship, where the information is necessary and proportionate to assess risk of fraud, scam, personal harm, financial loss or other wrongdoing; or
 - (c) KYC/AML or commercial due diligence: the Report is required for lawful KYC, AML, sanctions, anti-fraud, counterparty, beneficial-owner, officer, director, vendor, investor, intermediary, introducer or position-of-trust due diligence, and not for any FCRA-regulated or other prohibited purpose.
- 6.2.** Where you select personal or business risk assessment, you may be asked to select one sub-category: (a) online relationship, dating, virtual relationship or similar personal relationship risk; (b) investment opportunity, online offering, messaging-based proposal or suspected investment scam risk; (c) business relationship, commercial counterparty, supplier, introducer, intermediary or similar business risk; (d) family, personal safety or similar concern involving an adult only; or (e) other.

6.3. Where more than one purpose applies, you must select the main purpose and, where requested, briefly explain the additional context. Where you select “other” as a purpose, sub-category or recipient, or where your answers otherwise indicate a non-standard purpose, you must provide the further information requested and the Order will require SIP's review before acceptance.

6.4. Where requested, you must briefly describe the purpose of the Report, how you intend to use it, why the Report is necessary and proportionate for that purpose, and any additional context relevant to the selected purpose.

6.5. SIP does not provide legal advice. SIP's acceptance of an Order, or of any purpose information you provide, is not advice on, or approval or confirmation of, your lawful basis or your compliance with Applicable Data Protection Laws or any other law, for which you remain responsible.

7. Final pre-payment declaration

7.1. Before payment for each Fixed-Fee Report, you must confirm, by a mandatory affirmative action which may be presented as a single combined declaration, that:

- (a) you have selected the correct lawful purpose for the Report, and the Order is for a lawful, legitimate, specific, proportionate and documented purpose;
- (b) you do not know or suspect that the Subject is under 18, and if the requested Report relates to a person who is, or is believed to be, under 18, you must not order online and must contact SIP at client@sip-international.com for written approval before placing an Order;
- (c) you will not use the Report for employment, promotion, retention, reassignment, tenant screening, credit, insurance, housing, education, licensing, benefits, eligibility, harassment, stalking, doxxing, blackmail, intimidation, discrimination, unlawful surveillance or any other prohibited purpose;
- (d) you understand that the Report may contain inaccurate, incomplete, outdated, disputed or mismatched third-party information and is not legal, financial, tax, employment, credit, insurance, tenancy, safeguarding, AML/KYC compliance, security or other professional advice;
- (e) you will use, retain and disclose the Report only as permitted by these Terms and Conditions and only to Permitted Recipients where lawful, necessary, proportionate, confidential and consistent with the accepted Eligible Purpose;
- (f) you request SIP to begin performance immediately after payment and understand that cancellation and refund rights may be lost or limited once SIP begins work, incurs costs, accesses paid sources, undertakes analysis, processes the Order or makes the Report available; and
- (g) you agree to these Terms and Conditions and acknowledge SIP's Privacy Policy and Cookie Policy.

8. Order review, holds and refusals

8.1. Standard Orders may proceed through automated checkout where the confirmations required by this Schedule have been completed and none of the circumstances in paragraph 8.2 applies.

8.2. SIP may hold, decline or cancel an Order, prevent or suspend automated checkout, or require further information or written approval before acceptance or delivery, including where:

- (a) the Subject is, or may be, under 18;
- (b) a safeguarding, vulnerable-person, child-related, domestic abuse, harassment, stalking, intimidation or personal safety concern is indicated;
- (c) an employment, credit, insurance, tenant screening, housing, education, licensing, benefits, eligibility or other FCRA-regulated or similar use is indicated;
- (d) an “other” purpose, sub-category or recipient is selected;
- (e) you wish to disclose the Report to the Subject or to a person outside the categories in paragraph 5.1;
- (f) you decline to give a required confirmation, in which case the Order cannot be submitted;

- (g) sanctions, source, jurisdictional, reputational, legal, safety or misuse concerns arise; or
- (h) SIP otherwise considers review necessary before acceptance or delivery.

9. Payment and Report availability

9.1. The available service levels, the applicable fees and the total amount payable, including applicable taxes and fees, will be displayed on the Platform before payment. Payment for a Fixed-Fee Report is a one-time payment made in advance at checkout in accordance with clause 9 of these Terms.

9.2. You should download your Report promptly. Once first opened or accessed, the Report will be available on your dashboard for 14 days and will then be deleted from, or made inaccessible through, the dashboard. Unless a longer retention period is required or permitted for legal, regulatory, tax, accounting, audit, dispute, fraud prevention, security, safeguarding, insurance or compliance purposes, SIP will delete or anonymise Report files, Working Materials and Subject Data from its active systems within 60 days after delivery. SIP may retain limited account, order, invoice, payment, acknowledgement, audit and compliance records as described in these Terms and the Privacy Policy.

10. Safeguarding, minors and non-standard purposes

10.1. Online Fixed-Fee Report Orders must not be placed where the Subject is, or is believed to be, under 18. You must contact SIP at client@sip-international.com and obtain written approval before placing any such Order.

10.2. Any safeguarding, vulnerable-person or child-related purpose requires SIP's prior written approval and may be handled only as a Direct Service or otherwise as expressly approved by SIP in writing.

10.3. SIP may require evidence before accepting any such instruction, including evidence of authority, age band, safeguarding purpose, lawful basis, restricted-data condition, notices or exemptions, DPIA or risk assessment, and any relevant court, school, authority or legal documentation.

10.4. SIP may refuse or stop any child-related, safeguarding or non-standard instruction at any time where SIP believes the instruction is unsafe, unlawful, disproportionate, abusive, retaliatory, connected with harassment or domestic abuse, or otherwise inappropriate.