THIS AGREEMENT is dated [ ]

PARTIES:

(1) SECTA Research Limited, a company registered in England and Wales with company registration number 16213415, whose registered address is at Merlin Accountancy Services Ltd, 2nd Floor, 33 Longbrook Street, Exeter, England EX4 6AW ("**SECTA**")

(2) Subscribers to SECTA alerts (for the purposes of this agreement, "Subscribers", "Users" or "you"), identified by the information entered during the subscription process to SECTA communications.

each a "**party**" and together the "**parties**".

Background

(A) Sanctions Evasion & Circumvention Typologies Alerts (or SECTA) conducts intelligence-led, open-source investigations about sanctions evasions and circumvention. SECTA aims to share specific, relevant typologies with regulated entities to detect sanction evasion networks (the "**Services**").

(B) Subscribers in the UK or the EU agree to the terms in this Data Sharing Agreement ("Agreement") when receiving the email communications, or typologies, that make up the Services in this contract.

(C) The parties recognise that the provision of the Services involves the transfer and sharing of personal data. In light of this, the parties wish to enter into a data sharing agreement in accordance with the terms and conditions set out below.

Agreed Terms

1. Interpretation

1.1 In this Data Sharing Agreement, the following words and phrases shall have the following meanings (unless the context otherwise requires).

International Transfer Regulations	means UK regulations which set out in law that the legal framework of a particular country, territory or international organisation, or a particular sector in a country or territory has been assessed as providing protection for people's rights and freedoms relating to their personal data, such as to enable the free flow of data to that country, territory, organisation or sector.
Data Privacy Contact(s)	means an individual appointed by a party in accordance with clause 11.

Data Privacy Laws	means, as applicable, (i) the UK Data Protection Act 2018, (ii) the General Data Protection Regulation EU 2016/679 saved into UK law through section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") (iii) the Privacy and Electronic Communications Regulations 2003 and (iv) any other applicable enactment or rule of law relating to the processing of personal data and privacy (as amended, updated or superseded from time to time).
Data Security Breach	means a breach or breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Protected Data.
Data Sharing Agreement	means this agreement.
Data Subject(s)	means individuals whose personal data is shared among the parties to this Data Sharing Agreement.
Data Subject Request	means a request, notice or complaint made by, or on behalf of, a Data Subject in exercise of their rights under Data Privacy Laws relating to their Protected Data.
Particulars	means the description of the Protected Data, the Data Subjects and details of the transfer and sharing of the Protected Data amongst the parties, as set out in Schedule 1.
Protected Data	means the personal data to be processed by the parties in relation to this Data Sharing Agreement.
Purpose	has the meaning set out in Schedule 1.
UK ICO	means the UK Information Commissioner's Office as well as any successor body to the Information Commissioner's Office.

The terms **"controller"**, "**processor**", "**personal data**", "**processing**", and "**special category data"** and "**criminal offence data**" shall have the meanings given to them in the Data Privacy Laws.

2. The Roles of the Parties and Compliance with Laws

2.1 The parties acknowledge and understand that each party will act as an independent controller with respect to the Protected Data. Each party is entering into this Data Sharing Agreement in consideration of the other party complying with their respective obligations under this Data Sharing Agreement.

2.2 Each party will comply with its respective obligations under the Data Privacy Laws.

2.3 Each party shall use reasonable endeavours to ensure that it does not act or omit to act in a way as to cause another party to breach any of its obligations under Data Privacy Laws.

3. Sharing Protected Data

3.1 The parties acknowledge that they will share the Protected Data with each other in connection with the Purpose. Each party agrees as follows in respect of the Protected Data:

(a) each party will implement appropriate technical and organisational measures to safeguard Protected Data against any Data Security Breach. Such measures shall be proportionate to the harm which might result from any such Data Security Breach (and having regard to the nature of the Protected Data in question);

(b) each party will only access Protected Data necessary for its purposes and in accordance with the Purpose and shall process Protected Data for the Purpose (and in accordance with this Data Sharing Agreement), except with the prior written agreement of the other party;

(c) the parties will use reasonable efforts to ensure the Protected Data is accurate and up to date and transferred to the other party using a secure method of transfer;

(d) each party will ensure that its staff are properly trained and are aware of their responsibilities for any Protected Data that they have access to;

(e) when sharing Protected Data with third parties (including any data processors), each party shall ensure that appropriate risk assessments, due diligence and agreements are in place in connection with such sharing;

(f) each party will promptly notify any other party (within two (2) working days) if it receives a complaint or request relating to the other party's obligations under the Data Privacy Laws (other than a Data Subject Request, which is addressed in clause 5);

(g) on receipt of a notice under clause 3.1(f), each party will provide the other party with full co-operation and assistance in relation to any such complaint or request.

3.2 The parties will process the Protected Data in accordance with the Particulars set out in Schedule 1. The parties will apply the specific security measures to the Protected Data in accordance with Schedule 2.

4. Additional Measures for Sensitive Protected Data

4.1 Under this Data Sharing Agreement, the parties may share Protected Data which is criminal offence data.

4.2 In addition to the provisions in clause 3, each party agrees that with respect to the data set out in clause 4.1:

(a) this Protected Data is very sensitive personal data which may require additional measures to ensure its safety and security; and

(b) it will undertake its best efforts to ensure that criminal offence data is accurate and up to date and transferred to the other party using a secure method of transfer.

5. Data Subject Requests

5.1 Each party will ensure that it protects the rights of Data Subjects under the Data Privacy Laws and agrees to promptly notify the other party in writing (within three (3) working days) if it receives a Data Subject Request about personal data of a Data Subject that the other party is a controller of.

5.2 Each party agrees that the Data Subject Request will be dealt with by the party in receipt of the Data Subject Request, and that the other party will provide all reasonable co-operation and assistance in relation to any Data Subject Request to enable the party in receipt of the Data Subject Request to comply with such Data Subject Request within the relevant timescale set out in the Data Privacy Laws.

5.3 Each party in receipt of a Data Subject Request will ensure it responds to any such Data Subject Request adequately and in accordance with the Data Privacy Laws.

5.4 Where more than one party is named on a single Data Subject Request, the parties should nevertheless provide separate responses, but greater co-operation under clause 5.2 may be appropriate in the interests of costs and resources.

6. Notification of a Data Security Breach

6.1 Each party shall notify the other party without undue delay after becoming aware of any Data Security Breach involving the Protected Data and in any event no later than 24 (twenty-four) hours after becoming aware of the Data Security Breach.

6.2 Notices under clause 6.1 will (as far as reasonably possible) include a full description of:

(a) the nature of the Data Security Breach including details of the Protected Data and Data Subjects affected;

(b) the likely consequences of the Data Security Breach; and

(c) the measures taken or proposed to be taken by the affected party to address the Data Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.3 The party affected by the Data Security Breach will provide regular updates to the other party on the progress of the affected party's investigation into the Data Security Breach.

6.4 Each party shall provide reasonable assistance to the party affected by the Data Security Breach in the event that the affected party is required to notify the UK ICO, other regulator and/ or affected Data Subjects, in order to enable the affected party to comply with its obligations under the Data Privacy Laws.

7. **International Data Transfers**

7.1 No party may transfer Protected Data to any country outside the UK or EU unless that party ensures that (as required to comply with the Data Privacy Laws):

(a) the transfer is covered by International Transfer Regulations;

(b) there are appropriate safeguards in place as required by applicable Data Privacy Laws (including but not limited to appropriate due diligence and transfer risk assessment); or

(c) it can rely on a derogation from the relevant obligations under Data Privacy Laws.

8. **Retention and Deletion of Protected Data and Termination**

8.1 Each party agrees to only process the Protected Data for as long as reasonably necessary for the Purpose.

8.2 Nothing in this clause 8 will prevent either party from retaining and processing Protected Data in accordance with any statutory retention periods applicable to that party.

9. **UK ICO and Enforcement/ Court Action**

9.1 Where one party interacts with the UK ICO or other regulator (whether proactively, for example to review a data protection impact assessment or reactively, for example, in response to an inquiry from the UK ICO) in connection with the Protected Data, the other party will provide such information and assistance as is reasonably required to assist in such interactions.

9.2 In the event that any enforcement action is brought by the UK ICO or in the event of a claim brought by a Data Subject against either party, in both instances relating to the processing of Protected Data, the relevant party will promptly inform the other party about any such action or claim and will co-operate in good faith with the other party with a view to resolving it in a timely fashion.

10. **Changes to the Data Privacy Laws**

10.1 If during the term of this Data Sharing Agreement, the Data Privacy Laws change in a way that this Data Sharing Agreement is no longer adequate or appropriate for compliance with the Data Privacy Laws, the parties agree that they shall negotiate in good faith to review this Data Sharing Agreement in light of the current Data Privacy Laws and amend, terminate and/or replace this Data Sharing Agreement as appropriate.

11. **Data Privacy Contacts**

11.1 Each party will appoint a Data Privacy Contact in relation to the transfer of Protected Data under this Data Sharing Agreement. The first Data Privacy Contacts will be those set out in Schedule 3.

11.2 Any party may update its Data Privacy Contact by written notice to the other party.

11.3 Any notice to be provided under this Data Sharing Agreement is to be provided in writing to the relevant Data Privacy Contact(s). For the avoidance of doubt **in writing** includes email.

12. Counterparts

12.1 This Data Sharing Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts together shall constitute the one agreement.

13. Governing Law and Jurisdiction

13.1 This Data Sharing Agreement and any disputes or claims (including non-contractual disputes or claims) arising out of or in connection with its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

13.2 Each party irrevocably agrees that the courts of England and Wales have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement, its subject matter or formation.

[Signature Page Follows]

This Data Sharing Agreement is entered into by the parties on the date of the Subscriber’s agreement and subscription to SECTA alerts. Subscription to SECTA’s services constitutes the conclusion of this agreement.

Schedule 1 – Data Particulars

ITEM	DETAILS
Protected Data: personal data	The Protected Data includes: Information about staff and consultants of SECTA and Subscribers: ● Name ● Job title ● Contact details Information about potential actors of concern ● Name(s) ● Email address(es) ● Job title(s) ● Nationality(ies) ● Date of birth ● Physical address(es) ● Passport or ID number(s) ● Institutional or business affiliation(s) ● Telephone number(s) ● Social media account identifier(s) ● Messaging app account identifier(s) ● Bank account details ● Links to other natural persons, including family members ● Links to business or financial or trade transactions.
Protected data: special categories of personal data, criminal offence data, or otherwise sensitive data[1]	Information about potential actors of concern ● Criminal offence data.
Purpose of the sharing of Protected Data	The parties may share Protected Data to enable SECTA to provide the Services to Subscribers
Lawful bases for sharing the Protected Data under UK GDPR	The parties rely on the following lawful bases under Article 6 UK GDPR for sharing the Protected Data: ● Legitimate interests: The parties have a legitimate interest in sharing the Protected Data for the following purposes: detecting sanctions evasion schemes, ensuring compliance with sanctions regime. ● Legal obligation: The parties may need to process the Protected Data in order to comply with a legal obligation to which they are subject.

[1] **Special categories of personal data** include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. **Criminal offence data** includes personal data about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings.

ITEM	DETAILS
	The parties rely on the following lawful bases under Article 9 UK GDPR for sharing the Protected Data: ● Substantial public interest: The processing is necessary for reasons of substantial public interest. The parties rely on the following conditions under Schedule 1 of the Data Protection Act 2018: ● Preventing or detecting unlawful acts: The processing is necessary for the purposes of the prevention or detection of an unlawful act; ● Protecting the public against dishonesty: The processing is necessary for the exercise of a protective function (including dishonesty, malpractice or other seriously improper conduct); ● Regulatory requirements: The processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct.
Will the parties share the Protected Data with any other parties (Third Party/Parties)? (excluding processors)	The parties may disclose Protected Data to: ● their professional advisers including legal advisers; and ● any competent law enforcement body, regulatory, government agency, court or other third party where disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend legal rights.

Schedule 2 – Specific Security Measures

The following specific security measures will apply to the processing of the Protected Data by the parties:

1. The parties will ensure they maintain security measures to a standard appropriate to:

    (a) the risk to the rights and freedoms of the data subjects that might result from unlawful or unauthorised processing or accidental loss, alteration, disclosure, damage or destruction of Protected Data; and

    (b) the nature of the Protected Data.

2. The parties will maintain data security by protecting the confidentiality, integrity, availability and resilience of the systems processing Protected Data, where:

    (a) "confidentiality" means that only individuals who are authorised to use Protected Data can access it;

    (c) "integrity" means that Protected Data should be accurate and suitable for the purpose(s) for which it is processed;

    (d) "availability" means that Protected Data should be available to be accessed and used when required; and

    (e) "resilience" means that the systems processing Protected Data should be able to withstand threats and attacks.

3. In particular the parties shall:

    (a) have in place and comply with a security policy which:

        (i) defines security needs based on a risk assessment;

        (ii) allocates responsibility for implementing the policy to a specific individual;

        (iii) is disseminated to all relevant staff; and

        (iv) provides a mechanism for feedback and review;

    (f) ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Protected Data in accordance with best industry practice;

    (g) prevent unauthorised access to the Protected Data;

    (h) ensure storage of Protected Data conforms with best industry practice such that the media on which Protected Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Protected Data is monitored and controlled;

    (i) have secure methods in place for the transfer of Protected Data whether in physical form (for instance, by using couriers rather than post) or electronic form (for instance, by using encryption or pseudonymisation);

    (j) maintain password protection on computer systems on which Protected Data is stored and ensure that only authorised personnel are given details of the password;

(k) take reasonable steps to ensure the reliability of any employees or other individuals who have access to Protected Data;

(l) ensure that any employees or other individuals required to access Protected Data are informed of the confidential nature of Protected Data and comply with the obligations set out in this Agreement;

(m) have in place methods for detecting and dealing with Data Security Breaches (including loss, damage or destruction of Protected Data);

(n) provide all assistance reasonably required to enable the notification to the supervisory authority and/or a data subject of a Data Security Breach where this is required under the Data Privacy Laws;

(o) have a secure procedure for backing up and storing back-ups of Protected Data separately from originals;

(p) have an appropriate system in place to ensure that access to Protected Data can be restored in a timely manner in the event of any physical or technical incident;

(q) implement an effective system of regularly testing, assessing and evaluating the effectiveness of the measures used to ensure the security of the processing of Protected Data; and

(r) have a secure method of disposal for unwanted Protected Data including for back-ups, disks, print outs and redundant equipment.

Schedule 3 – Data Privacy Contacts

Data Privacy Contacts in relation to the data sharing are as follows:

For SECTA: Michael Lewis, Director, mlewis@sectaresearch.org