INTERNATIONAL DATA TRANSFER AGREEMENT

Between SECTA Research Limited and Subscriber (You)

This **Data Transfer 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**"); and

(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 outside the EU agree to the terms in this International Data Transfer 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 Transfer Agreement the following words and phrases shall have the following meanings (unless the context otherwise requires).

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 (**GDPR**), (iii) the GDPR as implemented into UK law (**UK GDPR**) (iii) the Privacy and Electronic Communications Directive 2002/58/EC (as implemented in national implementing legislation) and (iv) all other applicable laws and regulations relating to the processing of personal data and privacy (each as amended, updated and superseded from time to time).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 Subject(s)	means individuals whose personal data is shared among parties to this Data Transfer Agreement.
Data Subject Request	means an actual or purported 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.
Disclosing Party	means a party to this Data Transfer Agreement which is disclosing Protected Data to another party to this Data Transfer Agreement.
EEA	means the European Economic Area which comprises the countries of the European Union plus Norway, Iceland and Liechtenstein.
EU Adequacy Decision	A Decision of the European Commission on the basis of article 45 of GDPR that a country, territory or sector outside the EU or an international organisation provides an adequate level of data protection.
EU Model Clauses	the model contract for the transfer of personal data from controllers to controllers in third countries as set out under European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (Module One) in its current form, or as amended and updated.

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.
Model Clauses	means the EU Model Clauses and the UK Model Clauses.
Particulars	means the description of the Protected Data, the Data Subjects and details of the transfer and sharing of the Protected Data, as set out in Schedule 1.
Protected Data	means the personal data to be processed by the parties in relation to this Data Transfer Agreement.
Purpose	means provision of the Services by SECTA to Subscribers.
UK Model Clauses	means the UK addendum to the EU model clauses as set out in Schedule 5 in its current form, but which may be amended and updated.

1.2 The terms "**controller**", "**criminal offence data**", "**processor**", "**personal data**", "**processing**" and "**supervisory authority**" 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 a controller with respect to the Protected Data. The parties are each entering into this Data Transfer Agreement in consideration of the other parties complying with their respective obligations under this Data Transfer Agreement.

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

2.3 In the event that the Data Privacy Laws applicable to one party conflict with the Data Privacy Laws applicable to another party, the requirements of the country that necessitates stricter or additional requirements to protect Data Subjects' privacy and personal data shall be applied.

2.4 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.

2.5 For the avoidance of doubt, in the event of any conflict between the Model Clauses and the clauses in this Data Transfer Agreement, the Model Clauses shall take precedence.

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;

(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. The parties will process the Protected Data in accordance with the Particulars set out in Schedule 1.

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 relevant party in writing (within two (2) working days) if it receives a Data Subject Request for personal data of a Data Subject that the other relevant 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 relevant 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 the 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 A party affected by a Data Security Breach relating to the Protected Data shall notify the other party without undue delay after becoming aware of the Data Security Breach 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 its 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 party is required to notify a relevant supervisory authority, other regulator and/or affected Data Subjects.

7. **International Data Transfers**

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

(a) the transfer is covered by International Transfer Regulations or an EU Adequacy Decision (as relevant), including to the countries listed in Schedule 2 to this Data Transfer Agreement;

(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.

7.2 If a party carries out a transfer in circumstances referred to under clause 7.1 (b) the EU Model Clauses (and, as relevant, the UK Model Clauses) will apply to such a transfer, with the party based outside the UK/EEA acting as a **Data Importer** and the party based inside the UK/EEA acting as a **Data Exporter**.

7.3 If the Model Clauses are updated by the European Commission or by a UK authority (as appropriate), the parties shall apply the updated and amended form of the Model Clauses as required, without requiring further contractual agreements, unless the parties agree that another mechanism under Data Privacy Laws can be relied upon to provide appropriate protection for the Protected Data.

7.4 If the Model Clauses cease to be valid, whether by a decision of a court of competent jurisdiction, the European Commission or a UK authority (as relevant), the parties will co-operate in good faith to ensure that any continued transfers are compliant with the Data Privacy Laws.

7.5 For the avoidance of doubt, any Subscribers outside the EU are bound by the Model Clauses enclosed in this Agreement.

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 a party from retaining and processing Protected Data in accordance with any statutory retention periods applicable to that party.

9. **Relevant Authorities and Enforcement/Court Action**

9.1 Where one party interacts with any relevant supervisory authority (whether proactively, for example to review a data protection impact assessment or reactively, for example, in response to an inquiry from the supervisory authority), the other parties 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 a relevant supervisory authority 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**

If during the term of this Data Transfer Agreement, the Data Privacy Laws change in a way that this Data Transfer 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 Transfer Agreement in light of the current Data Privacy Laws and amend, terminate and/or replace this Data Transfer 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 Transfer Agreement. The Data Privacy Contact must be an individual

associated with the respective organisation with sufficient knowledge and experience of the Data Privacy Laws so as to be able to take decisions on behalf of that party in relation to this Data Transfer Agreement.

11.2 Each party will notify the other parties of the name, role and contact details of their Data Privacy Contact. Each party may update its Data Privacy Contact by written notice to the other parties.

11.3 Any notice to be provided under this Data Transfer 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**

This Data Transfer 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 Subject to any other provision in the Model Clauses, this Data Transfer 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 Subject to any other provision in the Model Clauses, 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.

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

Data Particulars and Security

Part 1 Data Particulars

ITEM	DETAILS
Protected Data	**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.
Special categories of personal data, criminal data, or otherwise sensitive data[1]	**Information about potential actors of concern** ● Criminal offence data.

[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 data** includes: personal data relating to criminal convictions and offences.

ITEM	DETAILS
Purpose of the transfer 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 (for EEA/ UK Members)	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, promoting compliance with national and international sanctions regimes. ● Legal obligation: The parties may need to process the Protected Data in order to comply with a legal obligation to which they are subject. The parties rely on the following lawful bases under Article 9/10 of the UK GDPR/Schedule 1 to 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.

Part 2 Specific Security Measures

The parties will comply with the following security measures set out in Annex 2 of Schedule 3 to this Agreement.

Schedule 2
Countries currently deemed adequate by the European Commission and/ or UK Government

Part 1 Countries deemed adequate by the European Commission:
Andorra; Argentina; Canada; Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United Kingdom, Uruguay.

Part 2 Countries deemed adequate by the UK Government:
All EEA Member States: Andorra; Argentina; Canada; Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, Uruguay.

Schedule 3
EU Model Clauses – Module One

SECTION I

1. Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[2] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

2. Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

3. Third-party beneficiaries

[2] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 – Clause 8.5 (e) and Clause 8.9(b);
(iii) Clause 12 – Clause 12(a) and (d);
(iv) Clause 13;
(v) Clause 15.1(c), (d) and (e);
(vi) Clause 16 (e);
(vii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

4. Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

5. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

6. Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

7. Docking Clause

(a) Not applicable.

SECTION II – OBLIGATIONS OF THE PARTIES

8. Data Protection Safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(viii) where it has obtained the data subject's prior consent;
(ix) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(x) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
  (i) of its identity and contact details;
  (ii) of the categories of personal data processed;
  (iii) of the right to obtain a copy of these Clauses;
  (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(e) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(f) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(g) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to

ensure compliance with this obligation, including erasure or anonymisation[3] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(h) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(i) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(j) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(k) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(l) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(m) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(n) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

[3] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

(a) The data importer shall not disclose the personal data to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

(b) Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

9. Left intentionally blank

10. Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[5] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

[5] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

11. Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
   (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

12. Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable

and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

13. Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

14. **Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[6];

[6] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

15. Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

---

with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

16. Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data

importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

17. **Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third party beneficiary rights. The Parties agree that this shall be the law of Ireland.

18. **Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX 1

A. LIST OF PARTIES

Data Exporter(s):

1. Name: SECTA Research Limited
   Address: Merlin Accountancy Services Ltd, 2nd Floor, 33 Longbrook Street, Exeter, England EX4 6AW
   Activities relevant to the data transferred under these Clauses: Processing: data of staff/consultants and potential actors of concern in order to provide the Services to Subscriber
   Role (controller/processor): Controller

Data Importer(s): As described in subscription sign-up form, if relevant (Subscriber outside the EU or UK)

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

- Staff/consultants of SECTA;
- Potential actors of concern

Categories of personal data transferred:

- Staff/consultants Information:
  - Name
  - Job title
  - Contact details
- 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.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures):

Potential actors of concern:

- Criminal offence data.

Applied restrictions/Safeguards

- Technological measures: Pseudonymisation, where appropriate; data minimisation (not retaining more data than required for the legitimate purposes set out above); not emailing data; password-protecting sensitive data.
- Data limitation (anonymising or pseudonymisation), in the interests of producing typologies rather than listing names of individuals

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

On a recurring basis, with the publication of SECTA typologies

Nature of the processing:

Sharing typologies of potential actors of concern in accordance with the provision of the Services.

Purpose(s) of the data transfer and further processing:

The parties will process the data in accordance with the provision of the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Personal data will be retained for as long as necessary for the relevant activity.

Retention periods will be based on the following criteria: (i) the respective statutory retention period; (ii) contractual and/or business relationships with data subjects; (iii) (potential) disputes; and (iv) any guidelines issued by relevant regulators. After expiration of that period, the relevant information will be

deleted, as long as it is no longer necessary for the fulfillment of a contract, the initiation of a contract or to protect or defend our position or that of a third party.

C. COMPETENT SUPERVISORY AUTHORITY

The appropriate supervisory authority shall be the relevant authorities of the United Kingdom.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Measures of pseudonymisation

Ensuring integrity of data through quality analysis and thorough review of information in the Services

Limiting data to that required for the services (provision of typologies)

Manual approval of Subscribers to ensure legitimate interest

Encryption and security measures to protect data during storage

Ensuring staff are trained appropriately on data security and cybersecurity risks

Policies requiring data erasure when the data is no longer required for the Services

Schedule 4
International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start date	[insert same data as Data Transfer Agreement]	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: SECTA Research Ltd Main address (if a company registered address): Merlin Accountancy Services Ltd, 2nd Floor, 33 Longbrook Street, Exeter, England EX4 6AW Official registration number (if any) (company number or similar identifier): 16213415	As submitted when subscribing

Table 2: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☒ Exporter ☐ neither Party

Part 2 Mandatory Clauses:

Mandatory Clauses	Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.