DATA PROCESSING ADDENDUM

The purpose of this Data Processing Addendum (“**DPA”**) is to set out each party's obligations relating to the personal data processed by the parties pursuant to the agreement (“**Agreement**”) entered into between them and to which this DPA is attached and incorporated.

1. DEFINITIONS

Defined terms used in this DPA shall have the same meaning as given in the Agreement unless otherwise defined below.

Appropriate Safeguards	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;
Controller	means the entity which determines the purposes and means of the Processing of Personal Data;
Data Subject	means the identified or identifiable person to whom Personal Data relates;
Data Subject Request	means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
Data Protection Laws	means all laws and regulations, including with regards to the processing of Personal Data to which a party is subject, including laws and regulations of the European Union, the European Economic Area and their member states, the UK’s Data Protection Act 2018 and the GDPR;
GDPR	means the General Data Protection Regulation (EU) 2016/679;
International Recipient	has the meaning given to that term in clause 7.1;
Personal Data	means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws;
Personal Data Breach	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;
Processor	means the entity which Processes Personal Data on behalf of the Controller;
processing	means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (and related terms such as **process** have corresponding meanings);

Processing Instructions	has the meaning given to that term in clause 3.2(a);
Protected Data	means Personal Data in Customer Data submitted to the Services or otherwise provided to Supplier by the Customer pursuant to the Agreement;
Services	means the services provided to Customer by Supplier pursuant to the Agreement and as defined therein;
Sub-Processor	means another Data Processor engaged by Supplier for carrying out processing activities in respect of the Protected Data on behalf of Supplier;
Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;
Working Day	means Monday to Friday inclusive excluding bank and public holidays in the UK.

2. ROLES AND OBLIGATIONS

2.1 Each party may collect and process Personal Data of the other as Controller for customer relationship management purposes and as such each party shall comply with all obligations of Controllers under Data Protection Laws in its processing of Personal Data for such purposes.

2.2 The parties agree that, for the Protected Data, Customer shall be the Controller and Supplier shall be the Processor.

2.3 Supplier shall process the Protected Data in compliance with:

(a) the obligations of Processors under Data Protection Laws; and

(b) the terms of this DPA.

2.4 Customer shall ensure all data it provides to Supplier for use in connection with the Services shall be collected and transferred to Supplier in accordance with Data Protection Laws. For the avoidance of doubt, it shall be Customer’s responsibility to (i) ensure the terms of use it supplies to the Data Subjects of the Protected Data comply with Data Protection Laws including in particular any fair processing information requirements relating to the processing of the Protected Data by Supplier and (ii) to ensure it has a legal basis for the processing of the Protected Data by Supplier.

3. INSTRUCTIONS

3.1 Customer shall, in its use of the Services, Process Protected Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions for the Processing of Protected Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Protected Data and the means by which Customer acquired Personal Data.

3.2 Insofar as Supplier processes Protected Data, Supplier:

(a) shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with Customer's documented instructions from time to time and in accordance with Annex 1 (Data Processing Particulars), as updated from time to time by written agreement of the parties or as otherwise detailed in the Agreement ("**Processing Instructions"**);

(b) shall inform Customer if Supplier is aware of a Processing Instruction that, in its opinion, infringes Data Protection Laws.

4. TECHNICAL AND ORGANISATIONAL MEASURES

4.1 Supplier shall implement and maintain:

(a) the technical and organisational measures prescribed by Data Protection Laws;

(b) taking into account the nature of the processing, the technical and organisational measures necessary to assist Customer insofar as is reasonably possible in the fulfilment of Customer's obligations to respond to Data Subject Requests relating to Protected Data.

5. SUB PROCESSORS AND STAFF

5.1 Supplier shall appoint its Sub-Processor(s) under a written contract containing materially equivalent obligations to those in this Data Processing Agreement. Details of such Sub-Processor(s) are set out in Annex 1 to this DPA.

5.2 Supplier shall ensure that all of its personnel and contractors processing Protected Data are subject to a binding written contractual obligation with Supplier or professional obligation to keep the Protected Data confidential (except where disclosure is required in accordance with applicable law, in which case Supplier shall, where practicable and not prohibited by applicable law, notify Customer of any such requirement before such disclosure).

5.3 Supplier may not change Sub-Processor without first notifying the Customer and giving the Customer ten days (from date of receipt of the notice) to object to the change in Sub-Processor on reasonable and objectively justifiable grounds. If Customer objects to the change in Sub-Processor, Supplier will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of the Protected Data by the objected to new Sub-Processor. If Supplier is unable to make available such change within a reasonable period of time, Customer may, by written notice, terminate those Services which cannot be provided by Supplier without the use of the objected to new Sub-Processor. Supplier will refund to Customer any prepaid fees covering the remainder of the term of such Services following the effective date of termination with respect to such terminated Services.

6. DATA SUBJECT REQUEST ASSISTANCE

6.1 Supplier shall promptly refer all Data Subject Requests it receives to Customer (wherever practicable within two Working Days of receipt of the request).

6.2 Supplier shall provide such assistance to Customer as Customer reasonably requires (taking into account the nature of processing and the information available to Supplier) to ensure compliance with each party's obligations under Data Protection Laws with respect to:

6.3 Data Subject Requests;

(a) security of processing;

(b) data protection impact assessments (as such term is defined in Data Protection Laws);

(c) prior consultation with a Supervisory Authority regarding high risk processing; and

(d) notifications to the Supervisory Authority and/or communications to Data Subjects by Customer in response to any Personal Data Breach and for the avoidance of doubt Supplier must promptly notify Customer in writing of any communications received by it from Data Subjects or Supervisory Authorities relating to the Protected Data without responding to either of the same unless it has been expressly authorised to do so by Customer.

6.4 Supplier shall be entitled to reimbursement of its reasonable costs for providing such notifications and assistance pursuant to sub-clause 6.2 above.

7. OVERSEAS TRANSFERS

7.1 To the extent required under Data Protection Laws, Supplier shall ensure that any transfers (and any onward transfers) of Protected Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws of the foregoing territories, are effected by way of Appropriate Safeguards and in accordance with such Data Protection Laws.

8. RECORDS AND AUDITS

8.1 Supplier shall maintain written records of all categories of processing activities carried out on behalf of Customer.

8.2 Supplier shall make available to Customer such information as is reasonably necessary to demonstrate its compliance with the obligations of Data Processors under Data Protection Laws, and shall allow for and contribute to audits, including inspections, by Customer (or another auditor mandated by Customer) for this purpose, subject to Customer:

(a) giving the Supplier at least 28 days' advance notice of such information request, audit and/or inspection being required; and

(b) Customer and Supplier mutually agreeing the scope, timing, and duration of the audit in addition to a reimbursement rate for Supplier's time and effort in co-operating with such audit, for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Supplier; and

(c) ensuring that all information obtained or generated by Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law). Customer shall provide a copy of such information and audit reports to Supplier following an inspection or audit pursuant to this clause 8.

9. BREACH NOTIFICATION

9.1 In respect of any Personal Data Breach involving Protected Data, Supplier shall without undue delay after becoming aware of the Personal Data Breach:

(d) notify Customer of the Personal Data Breach; and

(e) so far a possible without prejudicing the continued security of the Protected Data or any investigation into the Personal Data Breach, provide Customer with details of the Personal Data Breach.

10. DELETION OR RETURN OF DATA

10.1 Supplier shall either delete or return Protected Data to Customer in accordance with the provisions of the Agreement, unless storage of any data is required by applicable law and, if so, Supplier shall inform Customer of any such requirement and the period during which it is required to be stored.

11. LIABILITY

11.1 If a party receives a compensation claim from a person (including but not limited to a Data Subject) relating to processing of Protected Data processed by Supplier under this Agreement, it shall promptly provide the other party with notice and full details of such claim. Supplier shall make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of Customer.

11.2 This clause 11 does not affect the liability of Supplier to any Data Subject or Supervisory Authority pursuant to a claim made directly against Supplier by either of them.

11.3 As between Supplier and the Customer liability for all losses and damages arising out of any breach of this Data Processing Addendum including any arising from a Personal Data Breach, shall be governed by the limitations of liability and remedies for loss of data as set out in the Agreement.

Annex 1
Data processing PARTICULARS

1 Subject-matter of processing:

Correlation, verification and analysis of profile data relating to organisations and individuals as more particularly described in Service specifications.

2 Duration of the processing:

Subject to Clause 10 of this DPA, Supplier will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

3 Nature and purpose of the processing:

To use the Protected Data for the purpose of providing the Services and as otherwise detailed in the Agreement, and as further instructed by Customer in its use of the Services.

4 Type of Personal Data:

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Employment data (location, salary or salary band, reporting structure)
- Personal life data
- Connection data
- Localisation data

Special Category Data: None

5 Categories of Data Subjects:

Customer may submit Protected Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Protected Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's users authorized by Customer to use the Services

6 Processing Instructions

To use the Protected Data for the purpose of providing the Services and as otherwise detailed in the Agreement.

7 Sub-Processors

- **Google Cloud Platform (GCP)**, provided by Google Ireland Limited, with offices at Gordon House, Barrow Street, Dublin 4, Ireland. All PassFort services are currently hosted with Google Cloud Platform. As of today, PassFort only uses the Belgium datacenter of Google Cloud Platform, which guaranties that all data are stored within the EU.

- **C6 Intelligence Information Systems Limited**, 10 Queen Street Place, London EC4R 1BE, UK (company no. 05048084). Processing data to verify presence on Political Exposed Persons and International Sanctions lists, and on Adverse Media.

- **ComplyAdvantage**, provided by IVXS UK Ltd, whose registered office is at 8a Lower Grosvenor Place, London, SW1W 0EN (company no. 08964733). Processing data to verify presence on Political Exposed Persons and International Sanctions lists, and on Adverse Media.

- **Experian**, The Sir John Peace Building Experian Way NG2 Business Park, Nottingham NG80 1ZZ, UK (company no. 653331). Processing data to verify identity, addresses and identity documents such as passports or national ID cards.

- **GBG Group Plc (GBG)**, The Foundation, Herons Way, Chester Business Park, Chester CH4 9GB, UK (company no. 02415211). Processing data to verify identity, addresses and identity documents such as passports or national ID cards.

- **Jumio UK Limited**, 21 Worship Street, 3rd Floor, London EC2A 2DW, UK (company no. 10561447). Processing data to verify identity, addresses and identity documents such as passports or national ID cards.

- **Onfido Limited**, 40 Long Acre, London WC2E 9LG, UK. Processing data to verify identity, addresses and identity documents such as passports or national ID cards.

- **Regulatory DataCorp Limited (RDC)**, 10 Chiswell Street, London EC1Y 4UQ, UK. Processing data to verify presence on Political Exposed Persons and International Sanctions lists, and on media sources.

- **Trulioo**, 300 – 420 West Hastings Street, Vancouver, BC V6B 1L1, Canada. Processing data to verify identity, addresses and identity documents such as passports or national ID cards.