



## DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules and Appendices, (“DPA”) forms part of the Master Subscription Agreement or other written or electronic agreement between PassFort and Customer for the purchase of online services (including associated PassFort offline or mobile components) from PassFort, which includes the services listed on Appendix 3 to the Standard Contractual Clauses of this DPA (identified either as “Services” or otherwise in the applicable agreement, and hereinafter defined as “Services”) (the “Agreement”) to reflect the parties’ agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorised Affiliates, if and to the extent PassFort processes Personal Data for which such Authorised Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term “Customer” shall include Customer and Authorized Affiliates. All capitalised terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, PassFort may Process Personal Data on behalf of customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

### HOW TO EXECUTE THIS DPA

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, and 3 (including Appendices 1 to 3).
2. This DPA has been pre-signed on behalf of PassFort. The Standard Contractual Clauses in Schedule 3 have been pre-signed by PassFort Limited, as the data importer.
3. To complete this DPA, Customer must:
  - a. Complete the information in the signature box and sign on Page 9.
  - b. Send the signed DPA to PassFort by email to [dataprocessingaddendum@passfort.com](mailto:dataprocessingaddendum@passfort.com) indicating, if applicable, the Customer’s Account Number (as set out on the applicable PassFort Order Form or invoice).

Upon receipt of the validly completed DPA by PassFort at this email address, this DPA will become legally binding.

For the avoidance of doubt, signature of the DPA on page 9 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices. Where Customer wishes to separately execute the Standard Contractual Clauses and its Appendices, Customer should also complete the information as the data exporter on Page 14 and complete the information in the signature box and sign on Pages 20, 23 and 24.

## **HOW THIS DPA APPLIES**

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the PassFort entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with PassFort or its Affiliate pursuant to the Agreement, but it not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the PassFort entity that is party to such Order Form is party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

If the Customer entity signing this DPA is not a party to an Order Form not a Master Subscription Agreement directly with PassFort, but is instead a customer indirectly via an authorised reseller of PassFort services, this DPA is not valid and is not legally binding. Such entity should contact the authorised reseller to discuss whether any amendment to its agreement with that reseller may be required.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in Customer's Agreement (including any existing data processing addendum to the Agreement).

## **DATA PROCESSING TERMS**

### **1. DEFINITIONS**

**"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for the purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

**"Authorised Affiliate"** means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and PassFort, but has not signed its own Order Form with PassFort and is not a "Customer" as defined under this DPA.

**"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.

**"Customer"** means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.

**“Customer Data”** means what is defined in the Agreement as “Customer Data” or “Your Data”, provided that such data is electronic data and information submitted by or for Customer to the Services. This DPA does not apply to Content or Non-PassFort Applications as defined in the Agreement or, if not defined in the Agreement, as defined in the Master Subscription Agreement at <https://passfort.com/terms/>.

**“Data Protection Laws and Regulations”** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement.

**“Data Subject”** means the identified or identifiable person to whom Personal Data relates.

**“GDPR”** means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

**“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 and Regulations), where for each (i) or (ii) such data is Customer Data.

**“Processing”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**“Processor”** means the entity which Processes Personal Data on behalf of the Controller.

**“Security, Privacy and Architecture Documentation”** means the Security, Privacy and Architecture Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible via PassFort’s webpage at <https://passfort.com/terms/> or as otherwise made reasonably available by PassFort.

**“PassFort”** means the PassFort entity which is party to this DPA, as specified in the section “HOW THIS DPA APPLIES” above, being PassFort Limited, a company incorporated in England and Wales, United Kingdom.

**“PassFort Group”** means PassFort and its Affiliates engaged in the Processing of Personal Data.

**“Standard Contractual Clauses”** means the agreement executed by and between Customer and PassFort and attached hereto as Schedule 3 pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

**“Sub-processor”** means any Processor engaged by PassFort or a member of the PassFort Group.

**“Supervisory Authority”** means an independent public authority which is established by an EU Member State pursuant to the GDPR.

## **2. PROCESSING OF PERSONAL DATA**

**2.1. Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, PassFort is the Processor and that PassFort or members of the PassFort Group will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.

**2.2. Customer’s Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of PassFort as a Processor. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under GDPR.

**2.3. PassFort’s Processing of Personal Data.** PassFort shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions by the Customer (e.g. via email) where such instructions are consistent with the terms of the Agreement.

**2.4. Details of the Processing.** The subject-matter of Processing of Personal Data by PassFort is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Details of the Processing) to this DPA.

## **3. RIGHTS OF DATA SUBJECTS**

**Data Subject Request.** PassFort shall, to the extent legally permitted, promptly notify Customer if PassFort receives a request from a Data Subject to exercise the Data Subject’s right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a “Data Subject Request”. Taking into account the nature of the Processing, PassFort shall assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, PassFort shall upon Customer’s request provide commercially reasonable efforts to assist Customer in

responding to such Data Subject Request, to the extent PassFort is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from PassFort's provision of such assistance.

#### **4. PASSFORT PERSONNEL**

**4.1. Confidentiality.** PassFort shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. PassFort shall ensure. That such confidentiality obligations survive the termination of the personnel engagement.

**4.2. Reliability.** PassFort shall take commercially reasonable steps to ensure the reliability of any PassFort personnel engaged in the Processing of Personal Data.

**4.3. Limitation of Access.** PassFort shall ensure that PassFort's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

**4.4. Data Protection Officer.** Members of the PassFort Group have appointed a data protection officer. The appointed person may be reached at [privacy@passfort.com](mailto:privacy@passfort.com).

#### **5. SUB-PROCESSORS**

**5.1. Appointment of Sub-processors.** Customer acknowledges and agrees that (a) PassFort's Affiliates may be retained as Sub-processors; and (b) PassFort and PassFort's Affiliates may respectively engage third-party Sub-processors in connection with the provision of the Services. PassFort or an PassFort Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by each Sub-processor (unless the Sub-processor is a Non-PassFort Application with which the Customer has a separate Agreement and DPA in place and instructed PassFort to interoperate with).

**5.2. List of Current Sub-processors and Notification of New Sub-processors.** PassFort shall make available to Customer the current list of Sub-processors for the Services identified in Appendix 3 of the Standard Contractual Clauses attached hereto. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location ("**Infrastructure and Sub-processor Documentation**"). PassFort shall keep this Infrastructure and Sub-processor Documentation up to date and notify customers via it's webpage <https://passfort.com/terms/> of any changes.

**5.3. Objection Right for New Sub-processors.** Customer may object to PassFort's use of a new Sub-processor by notifying PassFort promptly in writing within thirty (30) days after receipt of PassFort's notice in accordance with the mechanism set out in Section 5.2. In the event the Customer objects to a new Sub-processor, as permitted in the preceding sentence, PassFort 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 Personal

Data by the objected-to new Sub-processor without unreasonably burdening Customer. If PassFort is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by PassFort without the use of the objected-to new Sub-processor by providing written notice to PassFort. PassFort will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

**5.4. Liability.** PassFort shall be liable for the acts and omissions of its Sub-processors to the same extent that PassFort would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

## 6. SECURITY

**6.1. Controls for the Protection of Customer Data.** PassFort shall maintain appropriate technical and organisational measures for protection of the security (including protection against unauthorised or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorised disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security, Privacy and Architecture Documentation. PassFort regularly monitors compliance with these measures. PassFort will not materially decrease the overall security of the Services during a subscription term.

**6.2. Third-Party Certifications and Audits.** PassFort has obtained third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, PassFort shall make available to Customer that is not a competitor of PassFort (or Customer's independent, third-party auditor that is not a competitor of PassFort) a copy of PassFort's then most recent third-party certifications, as applicable.

## 7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

PassFort maintains security incident management policies and procedures specified in the Security, Architecture and Privacy Documentation and shall notify the Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by PassFort or its Sub-processors of which PassFort becomes aware (a "**Customer Data Incident**"). PassFort shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as PassFort deems necessary and reasonable in order to remediate the cause of such Customer Data Incident to the extent the remediation is within PassFort's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

## 8. RETURN AND DELETION OF CUSTOMER DATA

PassFort shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Security, Privacy and Architecture Documentation.

## 9. AUTHORISED AFFILIATES

**9.1. Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorised Affiliates, thereby establishing a separate DPA between SFDC and each such Authorised Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorised Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorised Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services and Content by Authorised Affiliates must comply with the terms and conditions of the Agreement and any violation of the Agreement by an Authorised Affiliate shall be deemed a violation by Customer.

**9.2. Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with PassFort under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorised Affiliates.

**9.3. Rights of Authorised Affiliates.** Where an Authorised Affiliate becomes a party to the DPA with PassFort, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1. Except where applicable Data Protection Laws and Regulations require the Authorised Affiliate to exercise a right or seek any remedy under this DPA against PassFort directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right to seek any such remedy on behalf of the Authorised Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorised Affiliate individually but in a combined manner for itself and all of its Authorised Affiliates together (as set forth, for example, in Section 9.3.2., below).

9.3.2. The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on PassFort and its Sub-processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorised Affiliates in one single audit.

## 10. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to the DPA, and all DPAs between Authorised Affiliates and PassFort, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all the DPAs together.

For the avoidance of doubt, PassFort's and its Affiliates' total liability for all claims from Customer and all of its Authorised Affiliates arising out of or related to the Agreement and all DPAs established under the Agreement, including by Customer and all Authorised Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorised Affiliate that is a contractual party to any such DPA.

## **11. EUROPEAN SPECIFIC PROVISIONS**

**11.1. GDPR.** PassFort will Process Personal Data in accordance with the GDPR requirements directly applicable to PassFort's provision of its Services.

**11.2. Data Protection Impact Assessment.** Upon Customer's request, PassFort shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to PassFort. PassFort shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relation to section 11.2 of this DPA, to the extent required under the GDPR.

**11.3. Overseas data transfers.** PassFort ensures that any transfer of Personal 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 and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations, are effected by way of appropriate safeguards and in accordance with such Data Protection Laws.

## **12. PARTIES TO THIS DPA**

The Section "HOW THIS DPA APPLIES" specifies which PassFort entity is part of this DPA. Where the Standard Contractual Clauses are applicable, PassFort Limited, is the signatory to the Standard Contractual Clauses.

## **13. LEGAL EFFECT**

This DPA shall only become legally binding between Customer and PassFort when the formalities steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed.



The parties' authorised signatories have duly executed this DPA:

**CUSTOMER**

**PASSFORT LIMITED**

Signature:  
Entity Name:  
Print Name:  
Title:  
Date:

Signature:  
Print Name:  
Title:  
Date:

## SCHEDULE 1 – TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

### 1. ADDITIONAL TERMS FOR SERVICES

- 1.1. Customers covered by the Standard Contractual Clauses.** The Standard Contractual Clauses and the additional terms specified in this Section 3 apply to (i) Customer which is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom and, (ii) its Authorised Affiliates. For the purpose of the Standard Contractual Clauses and this Section 3, the aforementioned entities shall be deemed “data exporters”.
- 1.2. Instructions.** This DPA and the Agreement are Customer’s complete and final documented instructions at the time of signature of the Agreement to PassFort for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5 (a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Users in their use of the Services and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.
- 1.3. Appointment of new Sub-processors and List of Current Subprocessors.** Pursuant to Clause 5 (h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that (a) PassFort’s Affiliates may be retained as Sub processors; and (b) PassFort and PassFort’s Affiliates respectively may engage third-party Sub processors in connection with the provision of Services. PassFort shall make available to Customer the current list of Sub processors in accordance with Section 5.2 of this DPA.
- 1.4. Notification of New Sub-processors and Objection Right for new Sub-processors.** Pursuant to Clause 5 (h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that PassFort may engage new Sub-processors as described in Sections 5.2 and 5.3 of the DPA.
- 1.5. Copies of Sub-processor Agreements.** The parties agree that the copies of the Sub-processor agreements that must be provided by PassFort to Customer pursuant to Clause 5 (j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by PassFort beforehand; and, that such copies will be provided by PassFort, in a manner to be determined in its discretion, only upon request by Customer.
- 1.6. Audits and Certifications.** The parties agree that the audits described in Clause 5(f) and Clause 12 (2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Customer’s request, and subject to the confidentiality obligations set forth in the Agreement, PassFort shall make available to Customer that is not a competitor of PassFort (or Customer’s independent, third-party auditor that is not a competitor to PassFort) information regarding the PassFort Group’s compliance with the obligations set forth in this DPA in the form of third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation to the extent PassFort makes them generally available to its customers. Customer may contact PassFort in accordance with the “Notices” Section of the Agreement to request an on-site audit

of the procedures relevant to the protection of Personal Data. Customer shall reimburse PassFort for any time expended for any such on-site audit at the PassFort Group's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and PassFort shall mutually agree upon the scope, timing and duration of the audit in addition to the reimbursement rate for which the Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by PassFort. Customer shall promptly notify PassFort with information regarding any non-compliance discovered during the course of an audit.

**1.7. Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12 (1) of the Standard Contractual Clause shall be provided by PassFort to Customer only upon Customer's request.

**1.8. Conflict.** In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses shall prevail.

## **SCHEDULE 2 – DEATAILS OF THE PROCESSING**

### **Nature and Purpose of Processing**

PassFort will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

### **Duration of Processing**

Subject to Section 8 of the DPA, PassFort will Process Personal Data for the duration of the Agreement, unless otherwise provided in writing.

### **Categories of Data Subject**

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 Personal 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 authorised by Customer to use the Services

### **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
- Personal life data
- Localisation data

### **Special categories of data (if appropriate)**

Customer may, subject to the restrictions set out in the Documentation, submit special categories of Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which for the sake of clarity Personal Data with information 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 finances.

**SCHEDULE 3 – STANDARD CONTRACTUAL CLAUSES**

**Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation:

Address:

Tel:

E-mail:

Other information needed to identify the organisation:

.....

(the data **exporter**)

And

Name of the data importing organisation: PassFort Limited

Address: Mezzanine Floor, 24 Cornhill, London, EC3V 3ND, United Kingdom

Tel: +44 (0) 20 3633 1761

E-mail: [privacy@passfort.com](mailto:privacy@passfort.com)

Other information needed to identify the organisation: Not applicable

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

**Clause 1**

***Definitions***

For the purposes of the Clauses:

- a. *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor' 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- b. *'the data exporter'* means the controller who transfers the personal data;
- c. *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d. *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e. *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- f. *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## **Clause 2**

### ***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

## **Clause 3**

### ***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8 (2), and Clauses 9 to 12 as a third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5 (a) to (e) and (g), Clause 6, Clause 7, Clause 8 (2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor in this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8 (2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

#### **Clause 4**

##### ***Obligations of the data exporter***

The data exporter agrees and warrants:

- a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the provisions of that State;
- b. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable protection law and the Clauses;
- c. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- d. that after the assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and cost of their implementation;
- e. that it will ensure compliance with the security measures;
- f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g. to forward any notification received from the data importer or subprocessor pursuant to Clause 5 (b) and Clause 8 (3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- h. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub processing services which has to be made in



- accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i. that, in the event of sub processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
  - j. that it will ensure compliance with Clause 4 (a) to (i).

## **Clause 5**

### ***Obligations of the data importer***

The data importer agrees and warrants:

- a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b. that it has no reason to believe that legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- d. that it will promptly notify the data exporter about:
  - i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - ii. any accidental or unauthorised access, and
  - iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- e. to deal promptly and properly with all inquiries from the data exporter relating to its processing the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- f. at the request of the exporter to submit its data processing facilities for audit of the processing covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent member and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter , where applicable, in agreement with the supervisory authority;
- g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description

- of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- h. that, in the event of sub processing, it has previously informed the data exporter and obtained its prior written consent;
  - i. that the processing services by the subprocessor will be carried out in accordance with Clause 11;
  - j. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## **Clause 6**

### ***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such an entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or the data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

## **Clause 7**

### ***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

- b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

#### **Clause 8**

##### ***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take measures foreseen in Clause 5 (b).

#### **Clause 9**

##### ***Governing Law***

The clauses shall be governed by the law of the Member State in which the data exporter is established.

#### **Clause 10**

##### ***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

#### **Clause 11**

##### ***Subprocessing***

1. The data importer shall not subcontract any of its processing. Operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in la or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## **Clause 12**

### ***Obligation after the termination of personal data processing services***

1. The parties agree that on termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed on the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:.....

**On behalf of the data importer:**

Name (written out in full):

Position:

Address: Mezzanine Floor, 24 Cornhill, London, EC3V 3ND, United Kingdom

Other information necessary in order for the contract to be binding (if any):

Signature:.....

## **APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

### **Data exporter**

The data exporter is (please specify briefly your activities relative to the transfer):

Data Exporter is the legal entity specified in Section 3.1 of Schedule 1 of the DPA.

### **Data importer**

The data importer is (please specify briefly your activities relative to the transfer):

PassFort Limited is a provider of enterprise cloud computing solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

### **Data subjects**

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter 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
- Personal life data
- Localisation data

### **Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data, with information 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 or data concerning health.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing Personal Data by data importer is the performance of the Services pursuant to the Agreement.

DATA EXPORTER

Name:.....

Authorised Signature:.....

DATA IMPORTER

Name:.....

Authorised Signature:.....

**APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisation security measures implemented by the data importer in accordance with Clause 4 (d) and 5 (c) (or document/legislation attached):**

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services as described in the Security, Privacy and Architecture Documentation applicable to the Services purchased by data exporter, and accessible via <https://passfort.com/terms> otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the Services during a subscription term.

DATA EXPORTER

Name:.....

Authorised Signature:.....

DATA IMPORTER

Name:.....

Authorised Signature:.....



### **APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES**

- PassFort Services including:
  - Connect
  - Collect
  - Lifecycle
  - Policy Builder
  - Reporting