

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA

AGREEMENT TO BE ENTERED INTO BY OUTSYSTEMS AS PROCESSOR AND ITS SERVICES PROVIDER AS SUB-PROCESSOR

WHEREAS:

- A. Customer (hereinafter "Customer", the "Controller" or the "Company") has entered into a Master Subscription Agreement or into an agreement with similar nature and purpose (the "Master Agreement") with OutSystems (hereinafter "OutSystems" or the "Processor");
- B. Such Master Agreement entails the Processing of Personal Data by OutSystems on behalf of the Customer;
- C. OutSystems and Services Provider (hereinafter the "Services Provider" or the "Sub-Processor") have executed an agreement for the provision of certain Services (namely, and without limitation, a Consultancy Services Agreement, other type of Services agreement, an order form or purchased order or any other equivalent document, hereinafter the "Services Agreement");
- D. The execution of such Services Agreement and the provision of Services by the Services Provider entails the Processing of Personal Data on behalf of the Customer; and
- E. OutSystems and the Services Provider intend to regulate the Processing of Personal Data by the later on behalf of the Customer to the extent required by the applicable Data Protection Laws and by the Data Processing Agreement executed between such Customer and OutSystems.

OutSystems and the Services Provider (jointly referred to as "Parties") enter into this Data Processing Agreement, which is regulated by the following clauses:

1. DEFINITIONS

Capitalized terms shall have the meanings set out below. Any capitalized terms not defined below or elsewhere in this Data Processing Agreement shall have the meanings ascribed to them in the Services Agreement:

"Adequate Country" means a country or territory outside the EU/EEA that is recognized for the purposes of Data Protection Laws by virtue of a decision of the European Commission as providing an adequate level of protection for Personal Data, as defined by article 45 of the GDPR.

"Appropriate Safeguards" means any of the appropriate safeguards referred to in article 46 of the GDPR.

"Breach Event" means an event reasonably considered to be a "Data Breach", as defined on the GDPR, or otherwise involving the unauthorized and/or unlawful Processing of Personal Data whether in electronic, hard copy or other form including but not limited to malicious interference with information system operations by third parties.

"Controller" means the natural or legal person who determines the purposes and means of the Processing of Personal Data, who in this Data Processing Agreement is the Customer.

"Customer" means the Customer who has entered into the Master Subscription Agreement with OutSystems.

"Customer's Personal Data" means any Personal Data Processed by the Services Provider or another Sub-Processor on behalf of the Customer, as transmitted or given access to by OutSystems pursuant to or in connection with the Services Agreement.

"Data Subject" means the individual whose Personal Data is being Processed.

"Data Protection Laws" means all national, state, regional and/or local laws applicable to data privacy and to the Processing of "Personal Data" (defined below) including but not limited to, as applicable, the General Data Protection Regulation, (Regulation (EU) 2016/679) and the EU e-Privacy Directive (2002/58/EC) as may be amended by the proposed Regulation on Privacy and Electronic Communications, in each case as implemented into local laws applicable to the relevant Controller and/or Processor(s) with respect to the Personal Data (as relevant), any legislation that, in respect of a member state of EU, converts into domestic law the GDPR, the proposed Regulation on Privacy and Electronic Communications, or any other law relating to data protection, the Processing of Personal Data and privacy. The term Data Protection Laws shall be deemed to include any successor legislation or replacements for any of the laws referenced in this definition and includes all replacement laws and any similar laws governing the parties' activities in the European Union or any other applicable jurisdiction.

"EU/EEA" means European Economic Area.

"GDPR" means the EU General Data Protection Regulation 2016/679 and to the extent the GDPR is no longer applicable in the United Kingdom, any implementing legislation or legislation having equivalent effect in the United Kingdom. References to "Articles" or "Chapters" of the GDPR shall be construed accordingly.

"Personal Data" has the meaning as described on the applicable Data Protection Laws and shall include, without limitation, any data or information (regardless of the medium in which it is contained and whether alone or in combination) which may be supplied to or Processed by or on behalf of the Controller in connection with the provision of the Services, that relates to an identified or identifiable natural person ("Data Subject") including, without limitation, name, postal address, email

address, telephone number (in each case, as relevant to the particular Services), more particularly referred to in Exhibit A.

"Personnel" means the Services Provider's employees or other individuals with a contractual relationship with Services Provider.

"Process" has the meaning set out in the applicable Data Protection Laws, with respect to the description of Processing stated in Exhibit A, and includes any operation which is performed upon Personal Data, whether or not by automatic means, including but not limited to the access, acquisition, collection, recording, organization, storage, alteration, retrieval, consultation, use, disclosure, combination, transfer (including "Restricted Transfers", as defined below), blocking, return or destruction of Personal Data. **"Processed"** or **"Processing"** shall be construed accordingly.

"Processor" means the natural or legal person which processes Personal Data on behalf of the Controller.

"Restricted Transfers" means the transfer of Personal Data to a Third Country. Includes transfers from OutSystems of Customer's Personal Data to the Services Provider and onward transfers of Customer's Personal Data from a Sub-Processor to another Sub-Processor or between two establishments of a Sub-Processor. **"Transferred"** or **"Transferring"** shall be construed accordingly.

"Services" means the Services provided by the Services Provider to OutSystems as defined on the Services Agreement.

"Standard Contractual Clauses" means the Standard Contractual Clauses for the transfer of Personal Data to processors established in third countries, approved by the European Commission on a Decision dated as of 5 February 2010, as referred to by Exhibit C, which form part of this Data Processing Agreement and the Services Agreement which bind the Parties upon the signature of said Agreement.

"Sub-Processor" means an entity engaged by the Processor, exclusively for the Processing activities to be carried out as part of the Services on behalf of the Customer and in accordance with its instructions, as transmitted by OutSystems.

"Subsequent Sub-Processor" means an entity engaged by the Sub-Processor, or any other Subsequent Sub-Processor, exclusively for the Processing activities to be carried out as part of the Services on behalf of the Customer and in accordance with its instructions, as transmitted by OutSystems and by the Services Provider.

"Third Country" means a country or territory outside the EU/EEA that is not an "Adequate Country".

"User" means a natural person authorized by the Customer to use the Services.

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, OutSystems is the Processor and the Services Provider is the Sub-Processor.

2.2. Processing of Personal Data. The Services Provider shall Process Personal Data as confidential information and shall only Process Personal Data on behalf of the Customer and in accordance with the requirements of the Data Protection Laws, Customer and OutSystems' documented instructions and Exhibit A attached hereto, as necessary for the provision of the agreed Services by the Services Provider. Services Provider must inform the Customer and OutSystems immediately in case it believes that their instructions violate Data Protection Laws.

2.3. Details of the Processing. The subject-matter of Processing of Personal Data by the Services Provider is the performance of the Services pursuant to the Services Agreement. The nature and purpose of the Processing, the categories of Data Subjects and the types of Personal Data Processed under this Data Processing Agreement are further specified in Exhibit A to this Data Processing Agreement.

2.4. Duration of the Processing. The Processing shall be carried out for the duration of the Services Agreement, unless if otherwise agreed upon in writing.

3. SECURITY

3.1. The Services Provider uses appropriate technical, organizational and administrative security measures to protect the Personal Data Processed on behalf of the Customer and transmitted by OutSystems against accidental or unlawful loss, misuse, unauthorized access, disclosure, alteration and destruction. Services Provider's security measures are continually improved in line with technological developments.

3.2. The Services Provider has implemented access controls to ensure that the access and Processing of the Personal Data within the provision of the Services is strictly limited to those individuals who need to know or access such Personal Data for the performance of their specific duties or tasks (need-to-know).

3.3. Services Provider shall implement technical and organizational measures that ensure:

- (i) it will manage information and data security with reasonable efforts to restrict unauthorized access and will use best efforts to ensure that its Personnel are fully aware of the risks associated with information and data security issues;
- (ii) it utilizes encryption and other security technology to protect private information of the Controller from unauthorized access;

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA

(iii) that information and data under its responsibility is properly backed up on a daily basis and that arrangements for recovery processes are in place;

(iv) that proper measures are in place to enable continuation of Services, as far as reasonably possible, in case of the occurrence of an unexpected disruption event.

4. SERVICES PROVIDER'S PERSONNEL

4.1. Services Provider ensures that its Personnel who has access or processes Customers Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4.2. Upon OutSystems' or the Customer's request, as transmitted by OutSystems, the Services Provider shall provide evidence that its Personnel are subject to confidentiality, according with clause 4.1 above.

5. COOPERATION

5.1 Cooperation with the Customer and OutSystems. Services Provider shall fully cooperate with and assist both the Customer and OutSystems in relation to the response to any notifications from a supervisory authority, in connection with the Personal Data, including without limitation the preparation of supporting documentation to be submitted to the relevant supervisory authority and provision of supporting documentation sufficient to evidence that the Services Provider is legally bound by the terms of this Agreement.

In addition, Services Provider shall provide both Customer and OutSystems with all assistance and cooperation in the event of a Breach Event, namely in the preparation of the relevant notifications and in the implementation of the necessary mitigation measures.

Services Provider shall and shall procure that the Subsequent Sub-Processors shall promptly provide both to the Customer and OutSystems, upon request, all the information in its possession or control in relation to the Processing of the Personal Data under this Agreement and with all assistance and cooperation as may reasonably be required for Customer and OutSystems to assess whether its Processing of the Personal Data is in accordance with this Agreement.

The Services Provider shall cooperate fully with and assist the Customer and OutSystems in relation to any notifications or prior approvals that each of them may be required to effect or obtain from a supervisory authority, in connection with the Personal Data, including without limitation the preparation of supporting documentation.

5.2 Data Protection Impact Assessment and Prior Consultation.

Where requested to do so, the Services Provider shall make available the information reasonably required by the Customer or OutSystems to demonstrate its compliance with applicable Data Protection Laws and shall assist each of them to carry out a privacy impact assessment of the Services and work with each of them to implement agreed mitigation actions to address privacy risks identified.

5.3 Data Subject Requests. Services Provider shall, to the extent legally permitted, promptly notify both the Customer and OutSystems if it 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 ("Data Subject Request").

Considering the nature of the Processing, Services Provider shall assist both the Customer and OutSystems by applying appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customers' obligation to respond to a Data Subject Request under Data Protection Laws.

In addition, to the extent that Customer does not have the ability to address a Data Subject Request, the Services Provider shall upon Customer's request provide commercially reasonable efforts to assist the Customer in responding to such Data Subject Request, to the extent Services Provider is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations.

5.4 Authority Requests. Unless if prohibited by law, the Services Provider shall and shall procure that the Subsequent Sub-Processors shall promptly and in any event without undue delay notify both the Customer and OutSystems, including by providing copies, if it should receive any communication, correspondence or request for information (whether written or oral) from any regulatory or judicial authority relating directly or indirectly to the Personal Data, including in connection with any enforcement action or investigation under the Data Protection Laws.

5.5 Data Quality. The Services Provider shall and shall procure that the Subsequent Sub-Processors shall preserve the accuracy and integrity of Personal Data. The Services Provider shall update, amend, correct or delete Personal Data that is inaccurate or incomplete at Customer's or OutSystems' request, in accordance

with the provisions set forth in this Data Processing Agreement or under the Data Protection Laws.

Services Provider shall at all times promptly and fully cooperate with Customer's efforts to respond to any Data Subject inquiry or Breach Event response action requiring access to information stored or Processed by the Services Provider as requested by OutSystems on behalf of the Customer, without charging any additional costs to the Customer or to OutSystems.

5.6 Deletion, Destruction or Return of Personal Data. To the extent not otherwise prohibited by applicable Data Protection Laws, the Services Agreement or this Data Processing Agreement, notwithstanding any failure of the Customer or OutSystems to provide written instructions, Services Provider shall and shall procure that the Subsequent Sub-Processors shall delete or destroy upon termination of the Services Agreement, all Personal Data stored, collected or Processed on behalf of the Customer.

Following expiry or termination of the Services Agreement, and at any other time upon the Customer's or OutSystems' written request, the Services Provider shall and shall procure that all Subsequent Sub-Processors shall immediately and permanently delete all electronic copies of the Personal Data from its/their computer systems (including without limitation servers, hardware and mobile devices) and from digital media in its/their possession or control; and in respect of hard copies of the Personal Data, securely destroy all originals and copies of Personal Data in its, or its Subsequent Sub-Processors, possession, custody, or control.

Upon request, either from the Customer or from OutSystems the Services Provider shall provide a certification confirming that all Personal Data Processed under the Services Agreement has been securely destroyed.

5.7 Costs. Services Provider shall not charge any additional pricing in order to comply with its cooperation duties, referred to in this clause 5.

6. BREACH EVENT

6.1 Breach Notification. Services Provider shall notify OutSystems promptly and without undue delay but no later than within 24 hours after becoming aware of any actual or suspected Breach Event. Where and in so far as it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue delay.

6.2 Cooperation. Services Provider shall fully and promptly cooperate both with the Customer and OutSystems in satisfying its obligations with respect to a Breach Event, as determined by Data Protection Laws. The notification shall include:

- (i) a detailed description of the Breach Event, in particular, the categories and approximate number and identity of Data Subjects and Personal Data records concerned;
- (ii) any measure proposed to be taken to address the Breach Event and to mitigate its possible adverse effects; and
- (iii) all other information in its possession or control concerning the Breach Event.

Services Provider shall provide all assistance and cooperation as may be required for the Customer and OutSystems to mitigate the effects of the Breach Event, comply with the Data Protection Laws and adhere to guidance issued by relevant supervisory authority with regard to Breach Event management and reporting.

6.3 Investigation. Services Provider shall immediately investigate the Breach Event to identify, prevent and make best efforts to mitigate the effects of the Breach Event and subject to OutSystems prior agreement, to carry out any recovery or other action necessary to remedy the Breach Event.

6.4 Communication. Services Provider shall not release or publish any sort of communication regarding the Breach Event without Customer and OutSystems' prior written approval.

6.5 Costs. The actions referred to shall be undertaken at the expenses of the Services Provider, without prejudice to both Customer and OutSystems seek any legal remedy as a result of the Breach Event. Furthermore, Services Provider shall reimburse Customer and OutSystems of all costs, losses and expenses related to the management of the Breach Event.

7. SUBSEQUENT SUB-PROCESSORS

7.1 Selection of Subsequent Sub-Processors. Services Provider must choose Subsequent Sub-Processors that provide sufficient guarantees in respect of the technical security measures and organizational measures governing the Processing. The Subsequent Sub-Processors engaged must ensure compliance with the requirements and/or obligations foreseen in the Data Protection Laws and this Data Processing Agreement. Before the Subsequent Sub-Processor first Processes Personal Data on behalf of Customer and OutSystems, Services Provider must carry out due diligence to ensure that the Subsequent Sub-Processor is capable of providing the level of protection for Personal Data required by this Data Processing Agreement and Data Protection Laws.

7.2 Current Subsequent Sub-Processors. The Services Provider shall be entitled to engage Subsequent Sub-Processors for the

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA

Processing of Personal Data on behalf of the Customer, provided that OutSystems has given its prior and written consent. For these purposes, OutSystems expressly consents to the engagement as Subsequent Sub-Processors of the companies listed in Exhibit B, pursuant to article 28, paragraph 2, of the GDPR, and clause 11 of the Standard Contractual Clauses.

- 7.3 Objection.** The Services Provider shall notify in writing OutSystems in case of any changes concerning the addition or replacement of the Subsequent Sub-Processors listed on Exhibit B, giving OutSystems the opportunity to reasonably object to such change within 30 days after being notified. When notifying OutSystems, the Services Provider shall inform OutSystems of (i) the identification of the Subsequent Sub-Processor, (ii) the purpose of the Processing that will be carried out by such Subsequent Sub-Processor, (iii) the country where such company is located, (iv) the appropriate safeguards (in case of Restricted Transfers) and (v) if there will be onward transfers.

The Services Provider shall not transfer any Personal Data to the Subsequent Sub-Processor before the expiry of the 30 (thirty) days referred to in the precedent paragraph.

If, by any reason contrary to the willing of OutSystems, the Services Provider chooses an unsuitable Subsequent Sub-Processor that causes OutSystems to terminate the Agreement, then OutSystems is entitled to be indemnified for any damages caused, as referred to in Clause 11.

- 7.4 Engagement of Subsequent Sub-Processors.** With respect to each Subsequent Sub-Processor, the Services Provider shall ensure that the arrangement between the Services Provider and any prospective Subsequent Sub-Processor is governed by a written contract including terms which offer at least the same level of protection for the Personal Data as those set out in this Data Processing Agreement, and that such terms meet the requirements of Article 28, paragraph 3, of the GDPR and that Sub-Processors act in accordance with Customers' instructions, as transmitted by OutSystems.

- 7.5 Control of Subsequent Sub-Processors.** The Services Provider shall conduct periodically audits to the Subsequent Sub-Processors appointed that shall be documented and made available to OutSystems upon request.

- 7.6 Services Provider liability.** Where the Subsequent Sub-Processor fails to fulfil its data protection obligations, Services Provider will remain liable to Customer and to OutSystems for the performance of such Subsequent Sub-Processor obligations.

8. AUDIT RIGHTS

- 8.1 Information.** Services Provider shall and shall procure that any Subsequent Sub-Processor on request, makes available both to the Customer and OutSystems information reasonably necessary to demonstrate compliance with this Data Processing Agreement.

- 8.2 Audits.** Services Provider shall and shall procure that any Subsequent Sub-Processor allows the Customer and OutSystems to perform any audits in relation to the Processing of Personal Data under the Services Agreement which might include access to its premises by the Customer, OutSystems or an auditor mandated by each of them for this purpose.

The Customer and OutSystems shall give the Services Provider reasonable notice of any audit or inspection to be conducted under Section 8.2 and ensure that each of its mandated auditors uses its best efforts to avoid causing any damage, injury or disruption to the Services Provider premises, equipment, Personnel, data, and business while its Personnel and/or its auditor's Personnel (if applicable) are on those premises in the course any on-premise inspection.

9. RESTRICTED TRANSFERS

- 9.1** The Parties hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfers from OutSystems to the Services Provider.

The Standard Contractual Clauses shall come into effect on commencement of the relevant Restricted Transfers.

In the event of any conflict or inconsistency between this Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail when applicable.

The Services Provider agrees that no Personal Data Processed on behalf of the Customer shall be Processed by any Subsequent Sub-Processor outside the EU/EEA without OutSystems previous written consent and otherwise than in accordance with Chapter V of the GDPR. The Services Provider shall ensure that a legal mechanism to achieve adequacy in respect of that Processing is in place, such as (i) Sub-Processors' EU-US and Swiss-US Privacy Shield Framework certifications (if any), or (ii) Standard Contractual Clauses.

The Services Provider shall include in Exhibit B information regarding Restricted Transfers and inform OutSystems of any changes to the Appropriate Safeguards.

If any Subsequent Sub-Processor other than those referred to in Exhibit B is engaged by the Services Provider, pursuant to Clause 7 of this Agreement, the Services Provider shall inform OutSystems of the existence of any Restricted Transfers and the Adequate Safeguards adopted.

10. RECORDS

- 10.1** The Services Provider must keep records of its Processing activities performed on behalf of the Customer, as transmitted or given access to by OutSystems.

11. LIABILITY

- 11.1** Services Provider will indemnify and keep indemnified OutSystems against all and any loss, liability, damage and expenses (including reasonable legal fees) incurred by it as a result of any breach by Services Provider of its obligations under this agreement. Nothing contained herein shall be considered as prohibiting or limiting OutSystems from pursuing any other remedies available to it.

12. GOVERNING LAW AND JURISDICTION

- 12.1** This Data Processing Agreement shall be governed by, and construed and enforced in accordance with, the governing clause established in the Services Agreement, excluding the rules regarding the conflict of laws. In the absence of a governing clause, the governing law applicable to the OutSystems contracting party, as determined by the place of its registered office, shall prevail.

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA

EXHIBIT A PROCESSING ACTIVITIES

Brief description of the Processing activities	Purpose of the Processing	Categories of data subjects	Type of Personal Data
<p>The Services Provider will process Personal Data as necessary to perform the Services pursuant to the Services Agreement and applicable order(s). These Processing activities may include:</p> <ul style="list-style-type: none"> • Consulting and training Services related to the provision of any OutSystems proprietary Software. • Implementation or customization Services and/or advice related to the provision of any OutSystems proprietary Software. • Maintenance (e.g. testing and applying new product or system versions, patches, updates and upgrades, etc.) and support Services related to the provision of any OutSystems proprietary Software. 	<p>The purpose of the Processing is the provision of Services by the Services Provider pursuant to the Services Agreement and instructed by Processor on behalf of Controller in this Data Processing Agreement.</p>	<p>May include, as applicable, Personal Data relating to the following categories of data subjects:</p> <ul style="list-style-type: none"> • Customers, business partners and services providers of Controller (who are natural persons). • Employees or representatives of Controller's Customers, business partners and services providers (who are natural persons). • Employees, agents, advisors, contractors of Controller (who are natural persons). • Controller's users authorized by Controller to use the Services (who are natural persons). 	<p>Controller may submit Personal Data to the Services Provider, the extent of which is determined and controlled by Controller in its sole discretion, and which may include, as applicable, but is not limited to the following categories of Personal Data:</p> <ul style="list-style-type: none"> • Identification data (name). • Contact details (such as postal address, phone number and e-mail). • Professional data (such as job title and name of the company). • Contract data (information regarding the OutSystems Customer's order). • Usage data (such as data about the Customer's device and how such device interact with OutSystems and OutSystems' services). • Location data (such as location derived from the IP address or data that indicates where that Controller or Controller Customers' is located with less precision, such as at a city or postal code level). • Content data (such as the content of the Controller and Controller's Customers files and communications). • Credentials (such as passwords, passwords hints and similar security information used for authentication and account access to OutSystems' services).

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA**EXHIBIT B****PERMITTED AFFILIATES AND SUBSEQUENT SUB-PROCESSORS**

Sub-Processor	Purpose	Entity Country	Appropriate safeguards <i>(Only applicable to Restricted transfers)</i>	Onward Transfers <i>(Y/N)</i>
Non applicable.				

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA

EXHIBIT C

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 organization:

OutSystems, as identified in the Services Agreement in relation to which this Exhibit C forms part of and applicable order(s).

(the data **exporter**)

And

Name of the data importing organization:

The Services Provider, as identified in the Services Agreement in relation to which this Exhibit C forms part of and applicable order(s).

(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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 organizational security measures means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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), and (g)

- to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as 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 sub-processor 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 sub-processor 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 relevant 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 data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
- (d) that after 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, unauthorized 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 the 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 any sub-processor 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;

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA

- (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 sub-processor 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 the 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 organizational 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 unauthorized access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so.
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of 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 data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members 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 sub-processor will be carried out in accordance with Clause 11;

- (j) to send promptly a copy of any sub-processor 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 sub-processor is entitled to receive compensation from the data exporter for the 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 sub-processor 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 entity.
The data importer may not rely on a breach by a sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 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 sub-processor 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; and
 - (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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA

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

SUB-PROCESSING

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses.⁽³⁾. Where the sub-processor 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 sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor 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 law 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 sub-processor 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 the termination of the provision of data-processing Services, the data importer and the sub-processor 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 upon 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 sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Data exporter

The data exporter is:

OutSystems, which is an information technology company providing software products and services associated with its proprietary software, the OutSystems Platform.

Data importer

The data importer is:

The Services Provider, which will process personal data as necessary to perform the Services pursuant to the Services Agreement and applicable order(s).

Data subjects

The personal data transferred concern the following categories of data subjects:

- Customers, business partners and services providers of Controller (who are natural persons).
- Employees or representatives of Controller's Customers, business partners and services providers (who are natural persons).
- Employees, agents, advisors, contractors of Controller (who are natural persons).
- Controller's users authorized by Controller to use the Services (who are natural persons).

Categories of data

The personal data transferred concern the following categories of data:

- Identification data (name).
- Contact details (such as postal address, phone number and e-mail).
- Professional data (such as job title and name of the company).

- Contract data (information regarding the OutSystems Customer's order).
- Usage data (such as data about the Customer's device and how such device interact with OutSystems and OutSystems' services).
- Location data (such as location derived from the IP address or data that indicates where that Controller or Controller Customers' is located with less precision, such as at a city or postal code level).
- Content data (such as the content of the Controller and Controller's Customers files and communications).
- Credentials (such as passwords, passwords hints and similar security information used for authentication and account access to OutSystems' services).

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

Non-applicable.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

The Services Provider will process personal data as necessary to perform the Services pursuant to the Services Agreement and applicable order(s). These processing activities may include:

- Consulting and training Services related to the provision of any OutSystems proprietary Software.
- Implementation or customization Services and/or advice related to the provision of any OutSystems proprietary Software.
- Maintenance (e.g. testing and applying new product or system versions, patches, updates and upgrades, etc.) and support Services related to the provision of any OutSystems proprietary Software.

DATA PROCESSING AGREEMENT_EXHIBIT 1_CSA

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

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

The data importer uses appropriate technical, organizational and administrative security measures to protect the personal data transmitted by the data exporter against accidental or unlawful loss, misuse, unauthorized access, disclosure, alteration and destruction. Data importer's security measures are continually improved in line with technological developments.

The data importer has implemented access controls to ensure that the access and processing of the personal data is strictly limited to those individuals who need to know or access such personal data for the performance of their specific duties or tasks (need-to-know).

The data importer shall implement technical and organizational measures that ensure:

- (i) it will manage information and data security with reasonable efforts to restrict unauthorized access and will use best efforts to ensure that its Personnel are fully aware of the risks associated with information and data security issues;
- (ii) it utilizes encryption and other security technology to protect private information transferred by the Data Exporter from unauthorized access;
- (iii) that information and data under its responsibility is properly backed up on a daily basis and that arrangements for recovery processes are in place;
- (iv) that proper measures are in place to enable the processing of personal data, as far as reasonably possible, in case of the occurrence of an unexpected disruption event.