

**AMENDED AND RESTATED INTERCOMPANY AGREEMENT FOR TRANSFERS  
OF DATA BETWEEN MIMECASD ENTITIES**

## TABLE OF CONTENTS

	<u>Page</u>
<b>SECTION A – SCOPE OF THIS AGREEMENT.....</b>	<b>6</b>
<b>SECTION B –TRANSFERS BETWEEN DATA CONTROLLERS .....</b>	<b>8</b>
<b>SECTION C –TRANSFERS FROM A DATA CONTROLLER TO A DATA PROCESSOR .....</b>	<b>11</b>
<b>SECTION D – TRANSFERS FROM A DATA PROCESSOR TO SUB-PROCESSORS .....</b>	<b>14</b>
<b>SECTION E - TRANSFERS FROM A DATA PROCESSOR TO A DATA CONTROLLER.....</b>	<b>15</b>
<b>SECTION F – MISCELLANEOUS.....</b>	<b>16</b>
<b>SCHEDULE A PARTIES TO THIS AGREEMENT.....</b>	<b>22</b>
<b>SCHEDULE B DESCRIPTION OF TRANSFER .....</b>	<b>23</b>
<b>SCHEDULE C TECHNICAL AND ORGANISATIONAL SECURITY MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA.....</b>	<b>28</b>
<b>SCHEDULE D - 1 STANDARD CONTRACTUAL CLAUSES MODULE 1: CONTROLLER TO CONTROLLER TRANSFER .....</b>	<b>29</b>
<b>SCHEDULE D - 2 STANDARD CONTRACTUAL CLAUSES: UK (CONTROLLER TO CONTROLLER TRANSFER) .....</b>	<b>42</b>
<b>SCHEDULE E - 1 STANDARD CONTRACTUAL CLAUSES MODULE 2: CONTROLLER TO PROCESSOR TRANSFER .....</b>	<b>50</b>
<b>SCHEDULE E - 2 STANDARD CONTRACTUAL CLAUSES: UK (CONTROLLER TO PROCESSOR TRANSFER).....</b>	<b>63</b>
<b>SCHEDULE F STANDARD CONTRACTUAL CLAUSES MODULE 3: PROCESSOR TO PROCESSOR TRANSFER .....</b>	<b>71</b>
<b>SCHEDULE G STANDARD CONTRACTUAL CLAUSES MODULE 4: PROCESSOR TO CONTROLLER TRANSFER .....</b>	<b>85</b>
<b>SCHEDULE H DEED OF ADHERENCE.....</b>	<b>94</b>

**This Agreement** is made effective February 21, 2023 between the parties set out in Schedule A as amended from time to time (collectively, "Mimecast").

**Preamble:**

- (A) As a leading security, archiving and continuity cloud services provider with an ever-expanding global reach, Mimecast is committed to ensuring the safety and security of the personal data of its growing network of global customers.
- (B) In order to reinforce this commitment and help its customers comply with global regulations, Mimecast is implementing an extensive global data protection and security programme which will place the protection of personal data at the heart of its customer relationships.
- (C) By entering into this Agreement, Mimecast will ensure that adequate safeguards are in place with respect to the protection of its customer's personal data when transferred by Data Disclosers to Data Receivers.
- (D) In particular, Mimecast will enter into the standard contractual clauses approved by:
  - (i) in relation to transfers of Personal Data from the European Economic Area ("EEA"), the standard contractual clauses approved by Commission Decision 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679; and
  - (ii) in relation to transfer of Personal Data from the UK, the standard contractual clauses approved by Commission Decision of 27 December 2004 for the transfer of Personal Data to data controllers established in third countries and Commission Decision of 5 February 2010 for the transfer of Personal Data to data processors established in third countries, or any equivalent clauses issued by the relevant competent authority of the UK in respect of transfers of Personal Data from the UK;

in each case as amended, updated or replaced from time to time, as attached to and incorporated into this Agreement ("**Standard Contractual Clauses**") to cover data exports to Controllers or Processors as applicable established in Third Countries which do not ensure an adequate level of data protection;

- (E) In order to ensure compliance with the Standard Contractual Clauses across Mimecast's global business, the law governing Sections B, C and D of this Agreement will be determined by reference to the country in which the Data Discloser of the Personal Data is established, and the law governing Section E of this Agreement will be determined by the country in which the Data Receiver is established.

**Now it is hereby agreed** as follows:

**1. DEFINITIONS**

- 1.1 Unless expressly stated to the contrary or where the context requires otherwise, the following terms shall have the following meanings for the purposes of this Agreement:

"Personal Data", "Special Categories of Data/Sensitive Data", "Process/Processing", "Controller", "Processor", "Data Subject", and "Supervisory Authority" shall have the same meaning as in the relevant Applicable Data Protection Law;

"Applicable Data Protection Law" shall mean:

- (A) the General Data Protection Regulation 2016/679 (the "GDPR");
- (B) the Privacy and Electronic Communications Directive 2002/58/EC;

- (C) the UK Data Protection Act 2018 (“**DPA**”), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (“**UK GDPR**”), and the Privacy and Electronic Communications Regulations 2003; and
- (D) any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of personal data,

in each case as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time;

“**Data Discloser**” shall mean the Mimecast Entity who transfers the Personal Data to another Mimecast Entity;

“**Data Receiver**” shall mean the Mimecast Entity who agrees to receive from the Data Discloser Personal Data for further Processing in accordance with the terms of Section B (Transfers between Data Controllers), Section C (Transfers from a Data Controller to a Data Processor), Section D (Transfer to Sub-processors) or Section E (Transfer from a Data Processor to a Data Controller) of this Agreement;

“**Member State**” means the member states of the European Union from time to time;

“**Mimecast Entity**” means a party to this Agreement as set out in Schedule A (Parties to this Agreement) from time to time and “**Mimecast Entities**” means the collective parties to this Agreement as listed in Schedule A (Parties to this Agreement) from time to time;

“**Mimecast Services**” means Mimecast Services Limited, registered with company number 04901524, with registered address 1 Finsbury Ave, London EC2M 2PF, UK;

“**Relevant Data Export**” means:

- (A) a transfer of Personal Data:
  - (i) from a Mimecast Entity which is subject to Applicable Data Protection Law in respect of that Personal Data;
  - (ii) to another Mimecast Entity that is in a Third Country or a territory which otherwise (but for the operation of this Agreement) does not offer an adequate level of protection as required by Applicable Data Protection Law; and
  - (iii) which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law; and
- (B) the onward transfer of Personal Data transferred to a Mimecast Entity pursuant to (A) by that Mimecast Entity to a Third Country or a territory which otherwise (but for the operation of this Agreement) does not offer an adequate level of protection as required by Applicable Data Protection Law and which is not subject to any of the permitted derogations or conditions contained in Applicable Data Protection Law;

“**Services**” shall mean the email management service provided to end users of customers through a SaaS offering;

“**Security Standards**” shall mean the technical and organisational security measures set out in Schedule C; and

“**Third Country**” means (i) in relation to Personal Data transfers from the EEA, any country outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate

protection for Personal Data by the European Commission from time to time; and (ii) in relation to Personal Data transfers from the UK, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time.

- 1.2 References to a statutory provision include any subordinate legislation made from time to time under that provision.
- 1.3 References to this Agreement include the Schedules.
- 1.4 Headings shall be ignored in construing this Agreement.
- 1.5 If a word or phrase is defined, its other grammatical forms have a corresponding meaning.
- 1.6 The words “include”, “includes” and “including” and any succeeding words shall be construed without limitation to the generality of any preceding words or concepts.
- 1.7 If there is any inconsistency between the Clauses and Schedules to this Agreement, the Clauses shall take precedence.

## SECTION A – SCOPE OF THIS AGREEMENT

### 2. GENERAL

- 2.1 This Agreement governs the transfer of Personal Data between Mimecast Entities. This Agreement is divided into the following sections:
- (a) This Section A (Scope of this Agreement) provides a general overview of this Agreement;
  - (b) Section B (Transfers between Controllers) sets forth the terms governing any transfer (including a Relevant Data Export) from a Mimecast Entity acting as a Controller (e.g., an entity which alone or jointly with others determines the purposes and means of the processing of the relevant Personal Data), to another Mimecast Entity who is also acting as a Controller;
  - (c) Section C (Transfers from a Data Controller to a Data Processor) sets forth the terms governing any transfer (including a Relevant Data Export) from a Mimecast Entity acting as a Controller to another Mimecast Entity who is acting as a Processor on that Controller's behalf;
  - (d) Section D (Transfers from a Data Processor to a Sub-Processor) sets forth the terms governing any transfer (including a Relevant Data Export) from a Mimecast Entity acting as Data Processor to another Mimecast Entity acting as its sub-processor;
  - (e) Section E (Transfers from a Data Processor to a Data Controller) sets forth the terms governing any transfer (including a Relevant Data Export) from a Mimecast Entity acting as Processor on behalf of another Mimecast Entity acting as a Controller to that Controller Mimecast Entity;
  - (f) Section F (Miscellaneous) sets forth the general terms governing this Agreement.
- 2.2 The terms of this Agreement apply as between any Mimecast Entity which is party to this Agreement in its capacity as Data Discloser and any Mimecast Entity which is a party to this Agreement in its capacity as Data Receiver in relation to each transfer of Personal Data. Any Mimecast Entity which is a party to this Agreement may be Data Discloser and/or Data Receiver.
- 2.3 The Data Receivers have also entered into this Agreement to ensure that where a Data Receiver (i) receives personal data from any Data Discloser and onward transfers such personal data to another Data Receiver; or (ii) receives personal data from another Data Receiver which has been onward transferred, that Data Receiver is subject to contractual obligations to ensure such personal data is protected and to ensure compliance with this Agreement.
- 2.4 A new Data Discloser or a new Data Receiver may become a party to this Agreement by executing a deed of adherence in the form set out in Schedule H-1. Each of the Data Disclosers and the Data Receivers hereby irrevocably consent in advance to any such addition and acknowledges and agrees that any such addition shall be effective without any further consent from any Data Discloser or Data Receiver. Following such execution, the relevant new Data Discloser or new Data Receiver shall automatically become a party to this Agreement, on the date specified in the relevant deed of adherence. Each Data Discloser and Data Receiver undertakes to each new Data Discloser and new Data Receiver that from such date it shall observe, perform, and be bound by the provisions of this Agreement as though the relevant new Data Discloser or new Data Receiver were an original party to this Agreement.
- 2.5 A Data Discloser, and subject to the second sentence of this clause 2.5, a Data Receiver may withdraw from this Agreement at any time by giving a notice in the form set out in Schedule H-2 to Mimecast Services. A Data Receiver may only withdraw from this Agreement with consent from the Data Disclosers who transfer data to it and after it has ceased processing and deleted all personal data of such Data Disclosers. In addition, if any party ceases to be an affiliate of all other parties, it will be

deemed to have withdrawn from this Agreement from the date of cessation unless otherwise agreed with the other parties. The effect of any withdrawal will be to terminate this Agreement in respect of such party but will not affect this Agreement in so far as it relates to the other parties.

## **SECTION B –TRANSFERS BETWEEN DATA CONTROLLERS**

### **3. APPLICATION OF THIS SECTION B**

- 3.1 The parties agree that this Section B applies in each case and only where Personal Data is transferred from a Mimecast Entity acting as Controller to a Mimecast Entity acting as Controller.
- 3.2 The details of the transfers (as well as the Personal Data) covered by this Section B are specified in Schedule B which form an integral part of this Section B.
- 3.3 In the case of a Relevant Data Export to a Third Country outside of the EEA or the UK, as relevant, clause 7 shall govern the terms of the transfer and clauses 4, 5 and 6 shall not apply.

### **4. OBLIGATIONS OF BOTH PARTIES**

#### **4.1 Both the Data Discloser and Data Receiver:**

- (a) shall ensure that it processes the Personal Data fairly and lawfully; and
- (b) will:
  - (i) ensure that the Personal Data is accurate and up to date, and inform the other without undue delay if it becomes aware that any of the Personal Data is inaccurate or out of date;
  - (ii) provide reasonable assistance as necessary to the other to enable them to comply with subject access requests and to respond to any other queries or complaints from Data Subjects
  - (iii) carry out any reasonable request from the other to amend, transfer or delete any Personal Data (to the extent applicable);
  - (iv) notify the other promptly about any enquiries from the relevant Supervisory Authority in relation to the Personal Data and cooperate promptly and thoroughly with such Supervisory Authority, to the extent required under Applicable Data Protection Law; and
  - (v) notify Data Discloser promptly about any legally binding request for disclosure of 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.

- 4.2 Both the Data Discloser and Data Receiver warrant that they have no reason to believe that any applicable local laws, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Receiver from fulfilling its obligations under this Section B.

### **5. OBLIGATIONS OF THE DATA DISCLOSER**

#### **5.1 The Data Discloser warrants and undertakes that:**

- (a) the Personal Data have been collected, Processed, and transferred in accordance with the Applicable Data Protection Laws, as applicable, to the Data Discloser;
- (b) it has used reasonable efforts to determine that the Data Receiver is able to satisfy its legal obligations under this Section B;
- (c) the Data Discloser shall provide a copy of this Section B and its associated Schedules to the Supervisory Authority where required.



## **6. OBLIGATIONS OF THE DATA RECEIVER**

### **6.1 The Data Receiver warrants and undertakes that:**

- (a) it will have in place appropriate technical and organisational security measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the Processing and the nature of the data to be protected including those in the Security Standards, and shall ensure that those measures continue to provide an appropriate level of security;
- (b) in the event of a personal data breach, it shall take appropriate measures to address the personal data breach, and shall (if the breach is likely to result in a risk to individuals) notify the Data Discloser and cooperate with the Data Discloser in relation to any required notifications to the Supervisory Authority and/ or to relevant Data Subjects;
- (c) it will have in place procedures so that any third-party it authorises to have access to the Personal Data, including Processors, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the authority of the Data Receiver, including a Data Processor, shall be obligated to Process the Personal Data only on instructions from the Data Receiver. This provision does not apply to persons authorised or required by law or regulation to have access to the Personal Data;
- (d) it has no reason to believe, at the time of entering into this Section B, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under this Section B, and it will inform the Data Discloser (which will pass such notification on to the Supervisory Authority where required) if it becomes aware of any such laws;
- (e) it will inform the Data Discloser if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Section B;
- (f) it will Process the Personal Data for purposes described in Schedule B (Description of Transfer), and has the legal authority to give the warranties and fulfil the undertakings set out in this Section B;
- (g) it shall put in place appropriate technical or organisational measures in order to retain the Personal Data for no longer than necessary for the purposes for which it is processed;
- (h) it will process the Personal Data in accordance with Applicable Data Protection Laws of the country in which the Data Discloser is established; and
- (i) it will keep appropriate documentation of the Processing it carries out under this Section B, and shall make such documentation available to the Supervisory Authority.

## **7. TRANSFERS OUTSIDE OF THE EUROPEAN ECONOMIC AREA OR THE UK**

- 7.1 In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 1: Controller to Controller, set out in Schedule D-1, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser and the applicable Data Receiver for that particular transfer of personal data. In relation to any onward transfer of such personal data by that Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the Data Receiver obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 1: Controller to Controller set out in Schedule D-1; or (ii) the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E-1, in respect of that personal data.
- 7.2 In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses (Controller to Controller) set

out in Schedule D-2, which incorporate the provisions of Schedule B, and which together will form contractual terms between that Data Discloser and the applicable Data Receiver for that particular transfer of personal data. In relation to such onward transfer of the personal data by that Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the Data Receiver obligations set out in the Standard Contractual Clauses (Controller to Controller) set out in Schedule D-2 in respect of that personal data.

## **SECTION C – TRANSFERS FROM A DATA CONTROLLER TO A DATA PROCESSOR**

### **8. APPLICATION OF THIS SECTION C**

- 8.1 The parties agree that this Section C applies in each case and only where Personal Data is transferred from a Mimecast Entity acting as Controller to a Mimecast Entity acting as Processor.
- 8.2 The details of the transfers (as well as the Personal Data) covered by this Section C are specified in Schedule B which form an integral part of this Section C.
- 8.3 In the case of a Relevant Data Export to a Third Country outside of the EEA, or the UK, as relevant, clause 12 shall govern the terms of the transfer and clauses 9, 10 and 11 shall not apply.

### **9. OBLIGATIONS OF THE DATA DISCLOSER**

- 9.1 The Data Discloser agrees and warrants:
  - (a) it has used reasonable efforts to determine that the Data Receiver is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Section C;
  - (b) 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 Applicable Data Protection Law (and, where applicable, has been notified to the relevant authorities of the country in which the Data Discloser is established).
- 9.2 Both the Data Discloser and Data Receiver warrant that they have no reason to believe that any applicable local laws, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Receiver from fulfilling its obligations under this Section C.

### **10. OBLIGATIONS OF THE DATA RECEIVER**

- 10.1 The Data Receiver agrees and warrants:
  - (a) to Process the Personal Data only on documented instructions of the Data Discloser and this Agreement; if the Data Receiver cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Discloser of its inability to comply, including with regard to transfers of Personal Data to a Third Country or an international organisation, unless required to do so by European Union or Member State law or UK domestic law, as relevant, to which Data Receiver is subject. In such case, Data Receiver will inform Data Discloser of that legal requirement before Processing unless that law prohibits such information on important grounds of public interest;
  - (b) ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
  - (c) take all technical and organisational security measures including those in the Security Standards required in accordance with good industry practice and by Applicable Data Protection Law relating to data security, and shall ensure that those measures continue to provide an appropriate level of security;
  - (d) taking into account the nature of the Processing, assist Data Discloser by appropriate technical and organisational security measures, insofar as this is possible, for the fulfilment of Data Discloser's obligation to respond to requests for exercising the Data Subject's rights laid down in Applicable Data Protection Law;

- (e) notify (as applicable), and assist Data Discloser in ensuring compliance with data security, Personal Data Breach, data protection impact assessments, and engaging in other consultations, pursuant to Applicable Data Protection Law, taking into account the nature of processing and the information available to Data Receiver;
- (f) inform the Data Discloser without undue delay if it becomes aware that any of the Personal Data is inaccurate or out of date, and cooperate with the Data Discloser to erase or rectify the relevant Personal Data;
- (g) notify the Data Discloser promptly if it receives any legally binding request for disclosure of Personal Data by a public authority, or it becomes aware of any direct access to the Personal Data by public authorities, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. The Data Receiver shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. The Data Receiver will provide relevant information about disclosure requests to the Data Discloser, including in relation to its legality review and any challenges to the request;
- (h) inform the Data Discloser if it becomes aware of any applicable local laws that prevent it from fulfilling its obligations under this Section C;
- (i) at the choice of Data Discloser, promptly delete or return all the Personal Data to Data Discloser after the end of the provision of Services relating to Processing, and delete existing copies unless European Union or Member State law or UK domestic law, as relevant, requires storage of Personal Data;
- (j) keep appropriate documentation of the Processing it carries out under this Section C, and make available to Data Discloser (and any Supervisory Authority) all information necessary to demonstrate compliance with Applicable Data Protection Law (including the obligations laid down in Article 28 of the GDPR) and allow for and contribute to audits, including inspections, conducted by Data Discloser or another auditor mandated by Data Discloser; and
- (k) immediately inform Data Discloser if, in its opinion, an instruction infringes Applicable Data Protection Law.

## 11. SUB-CONTRACTING

- 11.1 The Data Discloser hereby consents to the use of the Subcontractors set out in <https://www.mimecast.com/company/mimecast-trust-center/> for the purposes further described therein. If Data Receiver appoints a new Subcontractor or intends to make any changes concerning the addition or replacement of the Subcontractors set out in <https://www.mimecast.com/company/mimecast-trust-center/>, it shall provide the Data Discloser with twenty business days' prior written notice, during which the Data Discloser can object against the appointment or replacement. If no Data Discloser objects, Data Receiver may proceed with the appointment or replacement. Data Receiver ensures that it has a written agreement in place with all Subcontractors which contains obligations on the Subcontractor which are no less onerous on the relevant Subcontractor than the obligations on Data Receiver under this Agreement (to the extent applicable to the Subcontractor). The Data Receiver shall remain fully responsible to the Data Discloser for the performance of any Subcontractor's obligations under its contract with the Data Receiver.
- 11.2 To the extent the Subcontractor is located in a Third Country, and in relation to a Relevant Data Export from the UK, Data Discloser hereby grants Data Receiver a mandate to enter into the Standard Contractual Clauses (Controller to Processor), set out in Schedule E-2, with such Subcontractor in its name and on its behalf.

**12. TRANSFERS OUTSIDE OF THE EUROPEAN ECONOMIC AREA OR THE UK**

- 12.1 In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 2: Controller to Processor set out in Schedule E-1, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser and the applicable Data Receiver for that particular transfer of personal data. In relation to any onward transfer of the personal data by that Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the Data Receiver obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 3: Processor to Processor set out in Schedule F; or (ii) the Standard Contractual Clauses – Module 4: Processor to Controller set out in Schedule G, in respect of that personal data.
- 12.2 In the case of a Relevant Data Export from the UK, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses (Controller to Processor) set out in Schedule E-2, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser and the applicable Data Receiver for that particular transfer of personal data. Each Data Discloser and Data Receiver agrees that the procedure in clause 11 shall apply to the granting of consent by each Data Discloser to the use of sub-processors as required under Clause 11 of the Standard Contractual Clauses (Controller to Processor) set out in Schedule E-2. In relation to any onward transfer of the personal data by that Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the Data Receiver obligations set out in the Standard Contractual Clauses (Controller to Processor) set out in Schedule E-2 in respect of that personal data.

## **SECTION D – TRANSFERS FROM A DATA PROCESSOR TO SUB-PROCESSORS**

### **13. APPLICATION OF THIS SECTION D**

- 13.1 The parties agree that this Section D applies in each case and only where Personal Data is transferred from a Mimecast Entity acting as Processor to a Mimecast Entity acting as sub-processor.
- 13.2 The details of the transfers (as well as the Personal Data) covered by this Section D are specified in Schedule B which form an integral part of this Section D.
- 13.3 In the case of a Relevant Data Export to a Third Country outside of the EEA, clause 16 shall govern the terms of the transfer and clauses 14 and 15 shall not apply.

### **14. OBLIGATIONS OF THE DATA DISCLOSER**

- 14.1 The Data Discloser agrees and warrants that it has used reasonable efforts to determine that the Data Receiver is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Section D.
- 14.2 Both the Data Discloser and Data Receiver warrant that they have no reason to believe that any applicable local laws, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Receiver from fulfilling its obligations under this Section D.

### **15. OBLIGATIONS OF THE DATA RECEIVER**

- 15.1 Data Receiver shall comply with the terms of Section C in relation to any such processing save that it acknowledges that the instructions from the Data Discloser will be based on the instructions received by the ultimate Data Controller and, accordingly, Data Receiver hereby agrees to comply with any additional instructions received from such Data Controller (either directly or via the Data Discloser) with respect to such sub-processing.

### **16. TRANSFERS OUTSIDE OF THE EUROPEAN ECONOMIC AREA**

- 16.1 In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 3: Processor to Processor set out in Schedule F, which incorporate the provisions of Schedule B and Schedule C, and which together will form contractual terms between that Data Discloser and the applicable Data Receiver for that particular transfer of personal data. In relation to any onward transfer of the personal data by that Data Receiver to another Data Receiver, the receiving Data Receiver shall comply with the Data Receiver obligations set out in, as applicable: (i) the Standard Contractual Clauses – Module 3: Processor to Processor set out in Schedule F; or (ii) the Standard Contractual Clauses – Module 4: Processor to Controller set out in Schedule G, in respect of that personal data.

## **SECTION E - TRANSFERS FROM A DATA PROCESSOR TO A DATA CONTROLLER**

### **17. APPLICATION OF THIS SECTION E**

- 17.1 The parties agree that this Section E applies in each case and only where Personal Data is transferred from a Mimecast Entity acting as Processor to a Mimecast Entity acting as Controller.
- 17.2 The details of the transfers (as well as the Personal Data) covered by this Section E are specified in Schedule B which form an integral part of this Section E.
- 17.3 In the case of a Relevant Data Export to a Third Country outside of the EEA, clause 19 shall govern the terms of the transfer and clauses 17 and 18 shall not apply.

### **18. OBLIGATIONS OF THE DATA DISCLOSER**

- 18.1 The Data Discloser agrees and warrants that it has used reasonable efforts to determine that the Data Receiver is able, through the implementation of appropriate technical and organisational measures, to satisfy its legal obligations under this Section E.
- 18.2 Data Discloser shall comply with the terms of clause 10 of Section C as applicable to a Data Receiver, in relation to any such processing.
- 18.3 [Both the Data Discloser and Data Receiver warrant that they have no reason to believe that any applicable local laws, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Receiver from fulfilling its obligations under this Section D.]

### **19. OBLIGATIONS OF THE DATA RECEIVER**

- 19.1 The Data Receiver agrees and warrants that the Processing of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of Applicable Data Protection Law (and, where applicable, has been notified to the relevant authorities of the country in which the Data Receiver is established).

### **20. TRANSFERS OUTSIDE OF THE EUROPEAN ECONOMIC AREA OR THE UK**

- 20.1 In the case of a Relevant Data Export from the EEA, the Relevant Data Export shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses – Module 4: Processor to Controller set out in Schedule G, which incorporate the provisions of Schedule B, and which together will form contractual terms between that Data Discloser and the applicable Data Receiver for that particular transfer of personal data.

## SECTION F – MISCELLANEOUS

### 21. COOPERATION WITH SUPERVISORY AUTHORITIES

- 21.1 The parties agree that they shall and, where applicable, shall procure that their representatives shall cooperate, on request, with the Supervisory Authority in the performance of its tasks pursuant to Applicable Data Protection Law.

### 22. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE SUPERVISORY AUTHORITY

In respect of any action or omission under this Agreement:

- (a) in the event of a dispute or claim brought by a Data Subject or the Supervisory Authority concerning the Processing of the Personal Data against either or both of the Data Receiver and/or the Data Discloser, the Mimecast Entities acting as Data Receiver and Data Discloser will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion;
- (b) the Mimecast Entities acting as Data Receiver and Data Discloser agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Supervisory Authority. If they do participate in the proceedings, the Mimecast Entities may elect to do so remotely (such as by telephone or other electronic means). The Mimecast Entities also agree to consider participating in any other arbitration, mediation, or other dispute resolution proceedings developed for data protection disputes; and
- (c) each Mimecast Entity shall abide by a decision of a competent court of the Data Discloser's country of establishment or of the Supervisory Authority which is final and against which no further appeal is possible.

### 23. LIABILITY

- 23.1 Each Mimecast Entity shall be liable to the other Mimecast Entities for damages it causes by any breach of this Agreement. Liability as between the parties is limited to actual damage suffered.
- 23.2 Each Mimecast Entity shall be liable to Data Subjects for damages it causes by any breach of third-party rights under this Agreement. This does not affect the liability of any party under Applicable Data Protection Law.

### 24. TERMINATION

- 24.1 In the event that the Data Receiver is in breach of its obligations under this Agreement, then the Data Discloser may temporarily suspend the transfer of Personal Data to the Data Receiver until the breach is repaired or this Agreement is terminated.
- 24.2 This Agreement shall terminate automatically upon the board of Mimecast Services passing a resolution to terminate this Agreement, in accordance with the terms of such resolution.
- 24.3 The Mimecast Entities, acting collectively, may terminate or rescind this agreement without the prior consent of any third-party.

### 25. NOTICES

- 25.1 Any notice given under this Agreement (a "Notice") shall be in writing and may be delivered personally or sent by first class post (and air mail if overseas) or by fax to the party due to receive the Notice to the usual or last known place of business of such party or to another person, address or fax number specified by that party by not less than 10 days' written notice to the other party received before the Notice was despatched.



25.2 Unless there is evidence that it was received earlier, a Notice is deemed given:

25.2.1 if delivered personally, when left at the address referred to above;

25.2.2 if sent by post (except airmail) two business days after posting it;

25.2.3 if sent by airmail, six business days after posting it;

25.2.4 if sent by fax, when clearly received in full.

**26. WAIVER**

Failure by any party to enforce its rights under this Agreement shall not be taken as or deemed to be a waiver of such right.

**27. ASSIGNMENT**

None of the Mimecast Entities may assign or transfer any of the rights or obligations under this Agreement without the prior written consent of the other Mimecast Entities, such consent not to be unreasonably withheld.

**28. VARIATIONS**

28.1 The Mimecast Entities may only amend or vary the terms of this Agreement with written consent of all of the Mimecast Entities.

28.2 The Mimecast Entities recognise that where an amendment or variation is made to this Agreement pursuant to this clause, the Mimecast Entities may need to make revised notifications to, or seek additional approval from local data protection regulators in order to comply with national privacy law.

**29. FURTHER ASSURANCES**

The Mimecast Entities will use their best endeavours to procure that any necessary third-party executes and performs all such further deeds, documents, assurances, acts and things as any of the parties to this Agreement may reasonably require by notice in writing to any other party to carry the provisions of this Agreement into full force and effect.

**30. INVALIDITY**

If any provision in this Agreement shall be held to be illegal, invalid or unenforceable in whole or in part, the legality, validity and enforceability of the remainder of this Agreement shall not be affected.

**31. ENTIRE AGREEMENT**

The Mimecast Entities agree that, to the extent any existing agreements between them relating to the Processing of Personal Data conflict with the provisions of this Agreement, such existing agreements shall terminate forthwith and shall immediately be superseded by the provisions of this Agreement. This clause shall be without prejudice to any accrued rights and liabilities under any existing agreements being superseded by operation of this clause. The parties also acknowledge that they have not been induced to enter into this Agreement by any representation, warranty or undertaking not expressly incorporated into it, provided that neither party is attempting to exclude any liability for fraudulent statements (including fraudulent pre-contractual misrepresentations on which the other party can be shown to have relied).

**32. COUNTERPARTS**

This Agreement may be entered into in any number of counterparts, all of which taken together shall constitute one and the same instrument.

**33. GOVERNING LAW**


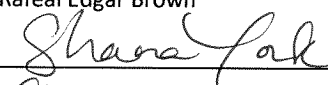
33.1 Subject to Clause 33.2, this Agreement shall be governed by English law.

33.2 The law governing Sections B (Transfers between Data Controllers), C (Transfers from a Data Controller to a Data Processor), D (Transfers from a Processor to a Sub-Processor) of this Agreement shall, in respect of each transfer, be the law of the country in which the Data Discloser is established. The law governing Section E (Transfers from a Processor to a Controller) of this Agreement shall, in respect of each transfer, be the law of the country in which the Data Receiver is established.


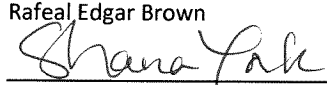
[REMAINDER LEFT INTENTIONALLY BLANK]

This Agreement has been executed and delivered as a deed on the date shown on the first page:

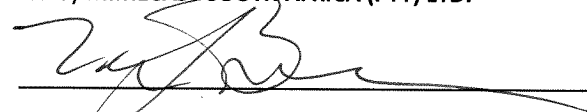
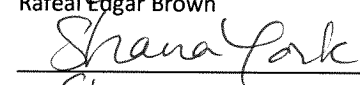
**EXECUTED as a deed by MIMICAST SERVICES LIMITED**

Signature:   
Director Name: Rafeal Edgar Brown  
Signature:   
Witness Name: Shana York

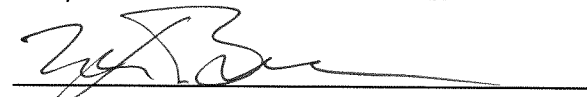
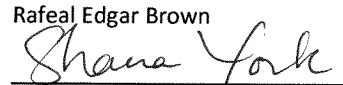
**EXECUTED as a deed by MIMICAST NORTH AMERICA, INC.**

Signature:   
Director Name: Rafeal Edgar Brown  
Signature:   
Witness Name: Shana York

**EXECUTED as a deed by MIMICAST SOUTH AFRICA (PTY) LTD.**

Signature:   
Director Name: Rafeal Edgar Brown  
Signature:   
Witness Name: Shana York

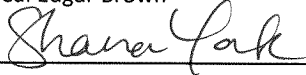
**EXECUTED as a deed by MIMICAST AUSTRALIA PTY LIMITED**

Signature:   
Director Name: Rafeal Edgar Brown  
Signature:   
Witness Name: Shana York

**EXECUTED as a deed by MIMICAST GERMANY GMBH**

Signature: 

Director Name: Rafeal Edgar Brown

Signature: 

Witness Name: Shana York

**EXECUTED as a deed by MIMICAST OFFSHORE LTD.**

Signature: \_\_\_\_\_

Director Name: \_\_\_\_\_

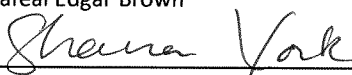
Signature: \_\_\_\_\_

Witness Name: \_\_\_\_\_

**EXECUTED as a deed by MIMICAST CANADA LIMITED**

Signature: 

Director Name: Rafeal Edgar Brown

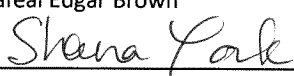
Signature: 

Witness Name: Shana York

**EXECUTED as a deed by MIMICAST ISRAEL LTD.**

Signature: 

Director Name: Rafeal Edgar Brown

Signature: 

Witness Name: Shana York

**EXECUTED as a deed by MIMICAST NETHERLANDS B.V.**

Signature: 

Director Name: Rafeal Edgar Brown

Signature: Shana York  
Witness Name: Shana York

**EXECUTED as a deed by MIMICAST SINGAPORE PTE LTD**

Signature: Rafeal Edgar Brown  
Director Name: Rafeal Edgar Brown  
Signature: Shana York  
Witness Name: Shana York

**EXECUTED as a deed by MIMICAST INDIA PRIVATE LIMITED**

Signature: Rafeal Edgar Brown  
Director Name: Rafeal Edgar Brown  
Signature: Shana York  
Witness Name: Shana York

**EXECUTED as a deed by MIMICAST FRANCE SARL**

Signature: Rafeal Edgar Brown  
Director Name: Rafeal Edgar Brown  
Signature: Shana York  
Witness Name: Shana York

**SCHEDULE A  
PARTIES TO THIS AGREEMENT**

<b>Company Name</b>	<b>Company Number (or equivalent)</b>	<b>Registered Address</b>
<b>Mimecast Services Limited</b>	04901524	Floor 4, 1 Finsbury Avenue, London, EC2M 2PF, UK
<b>Mimecast North America, Inc.</b>	5979597	191 Spring Street, Lexington, MA 02421 United States
<b>Mimecast South Africa (Pty) Ltd</b>	2004/000965/07	Upper Grayston Office Park, Phase 1 Block B, 150 Linden Road, Strathavon 2031 South Africa
<b>Mimecast Australia (Pty) Limited</b>	ACN: 161 990 512 ABN: 16 161 990 512	Level 3, 55 Southbank Boulevard, Southbank Vic 3006, Melbourne, Australia
<b>Mimecast Germany GmbH</b>	HRB234744	Kistlerhofstraße 172, 81379 München, Germany
<b>Mimecast Offshore Ltd.</b>	93944	22 Grenville Street, St Helier, Jersey, JE4 8PX
<b>Mimecast Canada Limited</b>	Incorp Number: BC1241412; Business Number: 746050277	Suite 2600, Three Bentall Centre, 595 Burrard Street, P.O. BOX 49314, Vancouver, BC, V7X 1L3, Canada
<b>Mimecast Israel Ltd.</b>	515058717	154 Menachem Begin Road, 18th Floor, Tel Aviv 6492107, Israel
<b>Mimecast Netherlands B.V.</b>	30214369	Stationsplein 12, 1211 EX Hilversum, The Netherlands
<b>Mimecast Singapore Pte Ltd.</b>	202200231N	9 Raffles Place #26-01 Republic Plaza, Singapore (048619)
<b>Mimecast India Private Limited</b>	U72900KA2022FTC167082	Helios Business Park, Level 06, Wing E, 150 Outer Ring Road, Kadubeesanahalli, Varthur Hobli, Bangalore - 560103, India
<b>Mimecast France SARL</b>	R.C.S.# - Paris 949 143 721	4 rue de Marivaux 75002 Paris, France

**SCHEDULE B  
DESCRIPTION OF TRANSFER**

**A. LIST OF PARTIES**

**Data exporter(s) - Controller:** *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: The relevant Mimecast Entity, as listed in Schedule A, who, acting as Data Controller, transfers the Personal Data to any other Mimecast Entity

Address: Addresses for all Group Entities are specified in Schedule A

Contact person's name, position, and contact details: Michael Paisley, Data Protection Officer, DPO@mimecast.com

Activities relevant to the data transferred under these Clauses: See section B (Description of Transfer) below.

Role (controller/processor): Controller

**Data exporter(s) - Processor:** *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: The relevant Mimecast Entity, as listed in Schedule A, who, acting as Data Processor, transfers the Personal Data to any other Mimecast Entity

Address: Addresses for all Group Entities are specified in Schedule A

Contact person's name, position, and contact details: Michael Paisley, Data Protection Officer, DPO@mimecast.com

Activities relevant to the data transferred under these Clauses: See section B (Description of Transfer) below.

Role (controller/processor): Processor

**Data importer(s) - Controller:** *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: The relevant Mimecast Entity, as listed in Schedule A, who, acting as Data Controller, agrees to receive Personal Data from the Data Discloser

Address: Addresses for all Group Entities are specified in Schedule A

Contact person's name, position, and contact details: Michael Paisley, Data Protection Officer, DPO@mimecast.com

Activities relevant to the data transferred under these Clauses: See section B (Description of Transfer) below.

Role (controller/processor): Controller

**Data importer(s) - Processor:** *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: The relevant Mimecast Entity, as listed in Schedule A, who, acting as Data Processor, agrees to receive Personal Data from the Data Discloser

Address: Addresses for all Group Entities are specified in Schedule A

Contact person's name, position, and contact details: Michael Paisley, Data Protection Officer, DPO@mimecast.com

Activities relevant to the data transferred under these Clauses: See section B (Description of Transfer) below.

Role (controller/processor): Processor

## **B. DESCRIPTION OF TRANSFER**

### *Categories of data subjects whose personal data is transferred*

Personal Data stored and processed in the provision of Mimecast Services may include data related to the following categories of Data Subjects:

- Employees, freelancers, contacts, third-party providers and contractors of Data Discloser's customers;
- Permitted/end users and other participants from time-to-time to whom the customer or partner has granted the right to access the Services in accordance with the customer or partner agreement with Data Discloser;
- End user customers of and individuals with whom those end-users communicate with by email and/or instant messaging;
- Service providers of the customers;
- Other individuals to the extent identifiable in the content of emails, other messaging services, their attachments, or in archiving content.

Personal Data held in furtherance of a business-to-business relationship of the Data Discloser may include the following categories of Data Subjects:

- Customers, prospect customers, agents, partners, prospect partners, vendors.

Personal Data held for marketing purposes may include data related to the following categories of Data Subjects:

- Customers and prospect customers of the Data Discloser.

### *Categories of personal data transferred*

- First and last name
- Job title
- Location data
- IP addresses, to the extent same may be used to identify a natural person
- Personal details, names, user names



- Identity card data
- Business and personal contact information e.g., phone number, address, email addresses of end users of the service
- Personal Data derived from the end users' use of the services such as records and reports
- Personal Data within email and other messaging content which identifies or may reasonably be used to identify Data Subjects
- Meta data including sent, to, from, date, time, subject, which may include Personal Data
- Images captured on security cameras relating to visitors to Mimecast's premises

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

No sensitive data or special categories of data are intended to be transferred, but, in the case of data stored and processed in the provision of the Mimecast services, sensitive data or special categories of data may be contained in the content of or attachments to email and/or other messaging - content which is not controlled by Mimecast.

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

Continuous and ongoing.

*Nature of the processing*

**The Personal Data transferred will be subject to the following basic Processing activities, where applicable (please specify):**

- Personal Data will be processed and stored to the extent necessary for the purposes set out below, which may include:
  - Human resources management and other required services related to operating our business throughout the course of the employment relationship, including recruitment administration and other required management of recruitment candidates.
  - Provision of Services. Personal Data will be Processed to the extent necessary to provide Services in accordance with the agreements with customers and other written Instructions.
  - Support. Technical support, issue diagnosis, and error correction to ensure the efficient and proper running of the systems to identify, analyse, and resolve technical issues both generally in the provision of the Services and specifically in answer to a customer query. This operation relates to all aspects of Personal Data Processed but will be limited to metadata where possible.
  - Threat Detection. As part of the Services, Mimecast Processes certain data reasonably identified to be malicious, including, without limitation, data which may perpetuate data breaches, malware infections, cyberattacks or other threat activity (collectively, "Threat Data"). Mimecast Processes Threat Data primarily through automated processes and may share limited Threat Data with third parties within

the cybersecurity ecosystem for the purpose of improving threat detection, analysis and awareness.

- Development and Improvement of Services. Primarily through automated processes designed to develop and improve our machine learning algorithms within Services, Mimecast Processes certain data that describes and/or gives information about customer data. "Machine-Learning Data" includes but is not limited to metadata, files, URLs, derived features, and other data. These machine-learning algorithms are hosted by Mimecast and/or Third-Party Subcontractors. The output of these machine learning algorithms is owned by Mimecast, does not contain customer data or personal data, and is anonymized and irreversible.
- Virus, anti-spam, and malware checking in accordance with the Services provided. This operation relates to all aspects of Personal Data Processed.
- URL scanning for the purposes of the provision of targeted threat protection and similar services which may be provided under agreements with customers. This operation relates to attachments and links in emails and will relate to any Personal Data within those attachments or links which could include all categories of personal information.
- Where personal customer data is stored and processed in the provision of the Mimecast services, access will be limited to that which is necessary to ensure the proper working of the systems and/or provide support to the customer and shall be appropriately logged.
- Personal Data held in furtherance of the business to business relationship between the customer or the partner and Mimecast or for marketing purposes will be processed as set out below, and may include:
  - Collection of Personal Data from Customers, prospect customers, partners, prospective partners, agents, consultants and vendors and thereafter inserting and storing the personal data in a centralized system that allows the Mimecast Entities to manage their business, financial, operational, customer, partner and vendor relations.
  - Providing intra-group marketing, business, and operational support.

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

**The transfer is made for the following purposes:**

- To enable efficient and effective business operations as follows:
  - To enable Mimecast entities to provide human resources management, customer, sales, marketing and engineering support to each of the other entities, customers and partners;
  - To ensure the proper working of the systems and services and to respond to support requests from customers and/or partners of Data Discloser; and
  - To enable a central database to be utilised to store and manage operational, marketing and business data and enable management of intra-group sales and marketing data.

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

As long as it is necessary to comply with data retention requirements, and with respect to customers, to provide customers with Services and successfully run the Mimecast business. Personal data may also be retained to (i) comply with legal or regulatory compliance needs (e.g., maintaining records of transactions made with Mimecast); (ii) to exercise, establish or defend legal claims; and/or (iii) to protect against fraudulent or abusive activity.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

As noted above in this Section B.

### **C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13 of Schedules D, E and F*

Bavarian Data Protection Authority (Bayerisches Landesamt für Datenschutzaufsicht)

Germany

**SCHEDULE C**  
**TECHNICAL AND ORGANISATIONAL SECURITY MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

Where applicable this Schedule C also forms part of the Standard Contractual Clauses.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

**Data Processor shall implement the technical and organisational security measures specified at <https://www.mimecast.com/company/mimecast-trust-center/> (or other suitable alternate measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the rights and freedoms of natural persons), as a minimum standard of security. Data Controller acknowledges and agrees that the nature of the Services mean that the technical and organisational measures may be updated by Data Controller from time-to-time but such updates shall not result in a lesser standard of security to that in place upon signature of this DPA.**

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

For transfers to sub-processors, technical and organisational measures will apply to safeguard the security and integrity of Personal Data that are no less protective than the obligations on Mimecast under the agreements with its customers in respect of the specific Services provided by the Third-Party Subcontractors.

**SCHEDULE D - 1**  
**STANDARD CONTRACTUAL CLAUSES MODULE 1: CONTROLLER TO CONTROLLER TRANSFER**

**SECTION I**

*Clause 1*

***Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)<sup>1</sup> for the transfer of personal data to a third country.
- (b) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

---

<sup>1</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

*Clause 3*

***Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 - Clause 8.5 (e) and Clause 8.9(b);
  - (iii) Clause 12 - Clause 12(a) and (d);
  - (iv) Clause 13;
  - (v) Clause 15.1(c), (d) and (e);
  - (vi) Clause 16(e);
  - (vii) Clause 18 - Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

***Hierarchy***

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

*Clause 6*

***Description of the transfer(s)***

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

*Clause 7 - Optional*

***Docking clause***

[Intentionally omitted]

**SECTION II – OBLIGATIONS OF THE PARTIES**

*Clause 8*

***Data protection safeguards***

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

### **8.1 Purpose limitation**

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

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

### **8.2 Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

- (i) of its identity and contact details;
- (ii) of the categories of personal data processed;
- (iii) of the right to obtain a copy of these Clauses;
- (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

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

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

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

### **8.3 Accuracy and data minimisation**

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

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

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

#### **8.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation<sup>2</sup> of the data and all back-ups at the end of the retention period.

#### **8.5 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

#### **8.6 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely

---

<sup>2</sup> This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.



identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

#### **8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union<sup>3</sup> (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

#### **8.8 Processing under the authority of the data importer**

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

#### **8.9 Documentation and compliance**

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

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

---

<sup>3</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

*Clause 9*

***Use of sub-processors***

*Clause 10*

***Data subject rights***

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.<sup>4</sup> The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- (b) In particular, upon request by the data subject the data importer shall, free of charge :
- (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
  - (ii) rectify inaccurate or incomplete data concerning the data subject;
  - (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the law of the country of destination, provided that such law lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
- (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
  - (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

---

<sup>4</sup> That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

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

#### *Clause 11*

##### ***Redress***

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### *Clause 12*

##### ***Liability***

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

*Clause 13*

***Supervision***

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

*Clause 14*

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

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in

light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>5</sup>;

- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

#### *Clause 15*

#### ***Obligations of the data importer in case of access by public authorities***

##### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if:
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred

---

<sup>5</sup> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

- (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### **15.2 Review of legality and data minimisation**

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

### **SECTION IV – FINAL PROVISIONS**

#### *Clause 16*

##### ***Non-compliance with the Clauses and termination***

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

- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### *Clause 17*

##### ***Governing law***

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

#### *Clause 18*

##### ***Choice of forum and jurisdiction***

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Germany.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX TO SCHEDULE D-1 (SCCS MODULE 1)**

**ANNEX I**

**A. LIST OF PARTIES**

*See Schedule B to the Intra-Group Agreement*

**B. DESCRIPTION OF TRANSFER**

*See Schedule B to the Intra-Group Agreement*

**C. COMPETENT SUPERVISORY AUTHORITY**

*See Schedule B to the Intra-Group Agreement*



**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

*See Schedule C to the Intra-Group Agreement*

**SCHEDULE D - 2**  
**STANDARD CONTRACTUAL CLAUSES: UK (CONTROLLER TO CONTROLLER TRANSFER)**

**Standard contractual clauses for the transfer of personal data from the Community to third countries  
(controller to controller transfers)**

*Data transfer agreement*

between

“**Data Exporter**” means the Data Discloser as defined in the Intra-Group Agreement, above.

hereinafter “data exporter”

and

“**Data Importer**” means the Data Receiver as defined in the Intra-Group Agreement, above.

hereinafter “data importer”

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

**Definitions**

For the purposes of the clauses:

- (a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);
- (b) “the data exporter” shall mean the controller who transfers the personal data;
- (c) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;
- (d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex 2, which forms an integral part of the clauses.

**I. Obligations of the data exporter**

The data exporter warrants and undertakes that:

- (a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.
- (b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.
- (c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

- (d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.
- (e) It will make available, upon request, a copy of the clauses to data subjects who are third-party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

## II. Obligations of the data importer

The data importer warrants and undertakes that:

- (a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
- (b) It will have in place procedures so that any third-party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.
- (c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.
- (d) It will process the personal data for purposes described in Annex 2, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.
- (e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).
- (f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).
- (g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a

regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

- (h) It will process the personal data, at its option, in accordance with:
  - (i) the data protection laws of the country in which the data exporter is established, or
  - (ii) the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or
  - (iii) the data processing principles set forth in Annex 1.

Data importer to indicate which option it selects: **(iii)**

Initials of data importer: **Signature of the Intra-Group Agreement or the Addendum under Schedule H shall be deemed selection of the indicated options.**

- (i) It will not disclose or transfer the personal data to a third-party data controller located outside the European Economic Area (EEA) or UK unless it notifies the data exporter about the transfer and
  - (i) the third-party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or
  - (ii) the third-party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or
  - (iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or
  - (iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

### **III. Liability and third-party rights**

- (a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third-party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.
- (b) The parties agree that a data subject shall have the right to enforce as a third-party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

#### **IV. Law applicable to the clauses**

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

#### **V. Resolution of disputes with data subjects or the authority**

- (a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
- (b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
- (c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

#### **VI. Termination**

- (a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.
- (b) In the event that:
  - (i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);
  - (ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;
  - (iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;
  - (iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or
  - (v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

- (c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector

thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

- (d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

#### **VII. Variation of these clauses**

The parties may not modify these clauses except to update any information in Annex 2, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

#### **VIII. Description of the Transfer**

The details of the transfer and of the personal data are specified in Annex 2. The parties agree that Annex 2 may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex 2 may, in the alternative, be drafted to cover multiple transfers.

## ANNEX 1 TO SCHEDULE D-2 (CONTROLLER–CONTROLLER SCCS)

### DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex 2 or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third-party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.
6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.
8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:
  - (a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

(ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

(b) where otherwise provided by the law of the data exporter.



**ANNEX 2 TO SCHEDULE D-2 (CONTROLLER-CONTROLLER SCCS)**

**DESCRIPTION OF TRANSFER**

*See Schedule B to the Intra-Group Agreement*

**SCHEDULE E - 1**  
**STANDARD CONTRACTUAL CLAUSES MODULE 2: CONTROLLER TO PROCESSOR TRANSFER**

**SECTION I**

*Clause 1*

***Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)<sup>6</sup> for the transfer of personal data to a third country.
- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

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

---

<sup>6</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

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

*Clause 3*

***Third-party beneficiaries***

- (e) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - (iii) Clause 9 - Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 - Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 - Clause 18(a) and (b).
- (f) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

**Hierarchy**

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

*Clause 6*

**Description of the transfer(s)**

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

*Clause 7 - Optional*

**Docking clause**

[Intentionally omitted]

**SECTION II – OBLIGATIONS OF THE PARTIES**

*Clause 8*

**Data protection safeguards**

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

**8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### **8.6 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>7</sup> (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

### **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

---

<sup>7</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

*Clause 9*

***Use of sub-processors***

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least twenty business days' in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.<sup>8</sup> The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*

***Data subject rights***

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

---

<sup>8</sup> This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

*Clause 11*

**Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

**Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.



*Clause 13*

***Supervision***

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

*Clause 14*

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

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in

light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>9</sup>;

- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

#### *Clause 15*

#### ***Obligations of the data importer in case of access by public authorities***

##### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred

---

<sup>9</sup> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

- (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### **15.2 Review of legality and data minimisation**

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

### **SECTION IV – FINAL PROVISIONS**

#### *Clause 16*

##### ***Non-compliance with the Clauses and termination***

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

- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### *Clause 17*

##### ***Governing law***

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

#### *Clause 18*

##### ***Choice of forum and jurisdiction***

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Germany.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX TO SCHEDULE E-1 (SCCS MODULE 2)**

**ANNEX I**

**A. LIST OF PARTIES**

*See Schedule B to the Intra-Group Agreement*

**B. DESCRIPTION OF TRANSFER**

*See Schedule B to the Intra-Group Agreement*

**C. COMPETENT SUPERVISORY AUTHORITY**

*See Schedule B to the Intra-Group Agreement*

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

*See Schedule C to the Intra-Group Agreement*

**SCHEDULE E-2**  
**STANDARD CONTRACTUAL CLAUSES: UK (CONTROLLER TO PROCESSOR TRANSFER)**

**Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)**

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 protection

between

**“Data Exporter”** means the Data Discloser as defined in the Intra-Group Agreement, above.

hereinafter “data exporter”

and

**“Data Importer”** means the Data Receiver as defined in the Intra-Group Agreement, above.

hereinafter “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 Annex 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 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 Annex 1 which forms an integral part of the Clauses.

#### *Clause 3*

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

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.

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.

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.

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 organisational security measures specified in Annex 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, 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 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;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex 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 organisational security measures specified in Annex 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 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 Annex 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.
3. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
4. 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;
  - (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).

*Clause 9*

**Governing law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the law of the country of the data exporter.

*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. 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, namely the law of the country of the data exporter.
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.

**ANNEX 1 TO SCHEDULE E-2 (CONTROLLER-PROCESSOR SCCS)**

**DESCRIPTION OF TRANSFER**

***See Schedule B to the Intra-Group Agreement***

**ANNEX 2 TO SCHEDULE E-2 (CONTROLLER-PROCESSOR SCCS)**

**TECHNICAL AND ORGANISATIONAL SECURITY MEASURES**

*See Schedule C to the Intra-Group Agreement*

**SCHEDULE F**  
**STANDARD CONTRACTUAL CLAUSES MODULE 3: PROCESSOR TO PROCESSOR TRANSFER**

**SECTION I**

*Clause 1*

***Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)<sup>10</sup> for the transfer of personal data to a third country.
- (e) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (f) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (g) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

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

---

<sup>10</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

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

*Clause 3*

***Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (ii) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (iii) Clause 8 - Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
  - (iv) Clause 9 - Clause 9(a), (c), (d) and (e);
  - (v) Clause 12 - Clause 12(a), (d) and (f);
  - (vi) Clause 13;
  - (vii) Clause 15.1(c), (d) and (e);
  - (viii) Clause 16(e);
  - (ix) Clause 18 - Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (c) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (d) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.



*Clause 5*

**Hierarchy**

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

*Clause 6*

**Description of the transfer(s)**

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

*Clause 7 - Optional*

**Docking clause**

[Intentionally omitted]

**SECTION II – OBLIGATIONS OF THE PARTIES**

*Clause 8*

**Data protection safeguards**

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

**8.1 Instructions**

- (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- (b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- (d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter<sup>11</sup>.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

---

<sup>11</sup> See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

### **8.3 Transparency**

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

### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### **8.6 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where

more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

### **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>12</sup> (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

### **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

---

<sup>12</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

#### *Clause 9*

#### ***Use of sub-processors***

- (a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least twenty business days' in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.<sup>13</sup> The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become

---

<sup>13</sup> This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*

**Data subject rights**

- (a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
- (b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

*Clause 11*

**Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

**Liability**

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

- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

#### *Clause 13*

#### ***Supervision***

- (a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.  
  
Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.  
  
Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

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

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>14</sup>;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

---

<sup>14</sup> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

#### *Clause 15*

#### ***Obligations of the data importer in case of access by public authorities***

##### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

##### **15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the



request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **SECTION IV – FINAL PROVISIONS**

##### *Clause 16*

##### ***Non-compliance with the Clauses and termination***

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without

prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*

**Governing law**

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

*Clause 18*

**Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Germany.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX TO SCHEDULE F (SCCS MODULE 3)**

**ANNEX I**

**A. LIST OF PARTIES**

*See Schedule B to the Intra-Group Agreement*

**B. DESCRIPTION OF TRANSFER**

*See Schedule B to the Intra-Group Agreement*

**C. COMPETENT SUPERVISORY AUTHORITY**

*See Schedule B to the Intra-Group Agreement*

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

*See Schedule C to the Intra-Group Agreement*

**SCHEDULE G**  
**STANDARD CONTRACTUAL CLAUSES MODULE 4: PROCESSOR TO CONTROLLER TRANSFER**

**SECTION I**

*Clause 1*

***Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)<sup>15</sup> for the transfer of personal data to a third country.
- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

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

---

<sup>15</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

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

*Clause 3*

***Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 - Clause 8.1 (b) and Clause 8.3(b);
  - (iii) Clause 15.1(c), (d) and (e);
  - (iv) Clause 16(e);
  - (v) Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

**Hierarchy**

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

*Clause 6*

**Description of the transfer(s)**

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

*Clause 7 - Optional*

**Docking clause**

[Intentionally omitted]

**SECTION II – OBLIGATIONS OF THE PARTIES**

*Clause 8*

**Data protection safeguards**

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

**8.1 Instructions**

- (a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- (b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- (c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- (d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

**8.2 Security of processing**

- (a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data<sup>16</sup>,

---

<sup>16</sup> This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or

the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

- (b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
- (c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### **8.3 Documentation and compliance**

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

#### *Clause 9*

#### ***Use of sub-processors***

#### *Clause 10*

#### ***Data subject rights***

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

#### *Clause 11*

#### ***Redress***

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

#### *Clause 12*

#### ***Liability***

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by

---

biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.



breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

#### *Clause 13*

#### ***Supervision***

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

#### *Clause 14*

#### ***Local laws and practices affecting compliance with the Clauses***

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>17</sup>;

---

<sup>17</sup> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal

- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

#### *Clause 15*

#### ***Obligations of the data importer in case of access by public authorities***

##### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

---

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

- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

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

## **SECTION IV – FINAL PROVISIONS**

### *Clause 16*

#### ***Non-compliance with the Clauses and termination***

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

- (ii) the data importer is in substantial or persistent breach of these Clauses; or
- (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

- (d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### *Clause 17*

##### ***Governing law***

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

#### *Clause 18*

##### ***Choice of forum and jurisdiction***

Any dispute arising from these Clauses shall be resolved by the courts of Germany.

**APPENDIX TO SCHEDULE G (SCCS MODULE 4)**

**ANNEX I**

**A. LIST OF PARTIES**

*See Schedule B to the Intra-Group Agreement*

**B. DESCRIPTION OF TRANSFER**

*See Schedule B to the Intra-Group Agreement*

**SCHEDULE H**  
**Deed of Adherence**

On [DATE OF AGREEMENT], Mimecast Services Limited and certain of its affiliates entered into a data export agreement (the “**Agreement**”). Capitalised terms used in this notice have the meanings given in the Data Export Agreement.

[JOINING AFFILIATE COMPANY] (the “**new [Data Discloser]/[Data Receiver]**”) is an affiliate of Mimecast Services Limited and wishes to enter into the Agreement, pursuant to clause [ ] of the Agreement. The new [Data Discloser]/[Data Receiver] confirms that it has been supplied with a copy of the Agreement and undertakes to each of the Data Disclosers and each of the Data Receivers that from [DATE] it shall observe, perform and be bound by the provisions of the Agreement as though it were an original party to the Agreement.

Notices to be sent to the new [Data Discloser]/[Data Receiver] under the Data Export Agreement will be sent to the following address (as the same may be changed from time to time by new [Data Discloser]/[Data Receiver] giving notice to Mimecast Services Limited):

[CONTACT DETAILS]

The ‘Point of Contact’ for the purpose of Schedule B of the Agreement shall be [NAME OF POINT OF CONTACT] at the following address: [ADDRESS].

*For UK Companies:*

Executed as a deed by [NAME OF EXECUTING COMPANY] acting by [NAME OF DIRECTOR], a director, in the presence of:

.....  
Director

.....  
Witness

.....  
Date

.....  
Name

.....

.....  
Address

.....  
Date

**OR**

*For non-UK companies:*

Signed as a deed by [NAME OF COMPANY], a company incorporated in [TERRITORY], acting by [NAME OF AUTHORISED SIGNATORY] [and [NAME OF AUTHORISED SIGNATORY]]:

.....  
Authorised Signatory

.....  
Date

.....  
[Authorised Signatory]

.....  
[Date]

**SCHEDULE H-2**

**WITHDRAWAL FROM THE AGREEMENT**

To: *[NAME OF RELEVANT CONTACT]*

On *[DATE OF AGREEMENT]*, Mimecast Services Limited and certain of its affiliates entered into a data export agreement (the "**Agreement**"). Capitalised terms used in this notice have the meanings given under the Agreement.

*[WITHDRAWING AFFILIATE COMPANY]* hereby gives notice, pursuant to clause [ ● ] of the Agreement, that it is withdrawing from the Agreement, effective as of *[DATE]*.

Signed by *[NAME OF DIRECTOR]*, a Director, for and on behalf of *[NAME OF COMPANY]*:

.....  
Director

.....  
Date