SOFTWARE AG CLICK WRAP DATA PROCESSING TERMS AND CONDITIONS

YOU SHOULD READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE ACCESSING AND/OR USING ANY SERVICES SPECIFIED IN THE AGREEMENT OF WHICH THESE CLICKWRAP DATA PROCESSING TERMS AND CONDITIONS FORM A PART ("**SERVICES**"). THE ACCESS AND/OR USE BY YOU OF ANY SERVICES WILL INDICATE YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS AND YOUR CONSENT TO BE BOUND BY THEM TOGETHER WITH YOUR ACKNOWLEDGEMENT OF YOUR AUTHORITY TO DO SO IN YOUR OWN RIGHT OR ON BEHALF OF YOUR COMPANY ("**CONTROLLER**") AND WILL CREATE A LEGALLY BINDING CONTRACT BETWEEN THE CONTROLLER AND SOFTWARE AG USA INC. ACTING IN ITS OWN NAME AND ACTING IN THE NAME AND ON BEHALF OF THE PROCESSORS LISTED IN APPENDIX 4 (EACH A "**PROCESSOR**"). IF YOU DO NOT AGREE WITH THESE SOFTWARE AG CLICK WRAP DATA PROCESSING TERMS AND CONDITIONS, YOU SHOULD NOT PROCEED WITH THE ACCESS AND/OR USE OF THE SERVICES.

PREAMBLE

WHEREAS, under the Agreement concluded between Processor and Controller, Processor agreed to provide Controller with the services as further specified in the Agreement and in Appendix 2 to this DPA (the "**Services**");

WHEREAS, the Parties agree that the bundling of the Processors (as listed in Appendix 4) within this single DPA is only undertaken for efficiency purposes (i.e. to avoid a multitude of different contract documents) and shall result in legally separate DPAs between the Controller and each Processor as designated in Appendix 4 and shall not create any legal or other relationship whatsoever between the bundled Processors other than between the Controller and each Processor separately;

WHEREAS, in rendering the Services, Processor may from time to time be provided with, or have access to information of Controller's end-customers or to information of other individuals having a (potential) relationship with Controller and this information may qualify as personal data within the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**") and other applicable data protection laws;

WHEREAS, Controller engages Processor as a commissioned processor acting on behalf of Controller as stipulated in Art. 28 GDPR;

WHEREAS, European data protection laws require controllers in EU/EEA countries to provide adequate protection for transfers of personal data to non-EU/EEA countries and such protection can be adduced by requiring processors to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries ("**Standard Contractual Clauses**") pursuant

to Commission Decision 2010/87/EU of 5 February 2010 as set out in Appendix 1;

WHEREAS, this DPA contains the terms and conditions applicable to the processing of such personal data by Processor as a commissioned data processor of Controller with the aim to ensure that the Parties comply with applicable data protection law.

In order to enable the Parties to carry out their relationship in a manner that is compliant with applicable law, the Parties have entered into the DPA as follows:

1 DEFINITIONS

1.1 For the purposes of this DPA, the terminology and definitions as used by the GDPR shall apply. In addition to that,

"Data Exporter"	shall mean the Controller, if (a) (i) the Controller is located in the EU/EEA or (ii) is located outside of the EU/EEA and is subject to the GDPR, and (b) transfers personal data to a Data Importer.
"Data Importer"	shall mean the Processor or Subprocessor that is located in a Third Country.
"**Member State**"	shall mean a country belonging to the European Union or to the European Economic Area.
"**Subprocessor**"	shall mean any further processor that is engaged by Processor as a sub-contractor for the performance of the Services or parts of the Services to be provided by Processor to Controller provided that such Subprocessor has access to the personal data of Controller when carrying out the subcontracted Services.
"**Third Country**"	shall mean a country outside of the EU/EEA that is not a White-List Country.
"White-List Country"	shall mean a country which is found by a decision of the EU Commission to ensure an adequate level of data protection within the meaning of Article 25 (2) of the Data Protection Directive (95/46/EC) and from May 25, 2018 within the meaning of Article 45 (1) General Data Protection Regulation.

1.2 This DPA has four Appendices. Appendix 1 contains the main body of the Standard Contractual Clauses. Appendix 2 contains the details of the processing and Appendix 3 contains the technical and organizational measures. Appendix 4 contains the list of processors. Appendix 2, Appendix 3 and Appendix 4 shall always apply. Appendix 1 shall apply in addition to this DPA only, if

(a) the Controller is located in the EU/EEA or is located outside of the EU/EEA and is subject to the GDPR, and

(b) the Processor is located in a Third Country. If Appendix 1 applies, Appendix 1 will prevail over this DPA in case of contradictions.

2 DETAILS OF PROCESSING

2.1 The details of the processing operations provided by Processor to Controller as a commissioned data processor (e.g., the subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects) are specified in Appendix

2 to this DPA.

3 OBLIGATIONS OF CONTROLLER

3.1 Controller is obliged to ensure compliance with any applicable obligations under the GDPR and any other applicable data protection law that applies to Controller as well as to demonstrate such compliance as required by Art. 5 (2) GDPR. Controller remains the responsible data controller for the processing of the personal data.

3.2 Controller is obliged to confirm before processing is carried out that the technical and organizational measures of Processor, as set out in Appendix 3, are appropriate and sufficient to protect the rights of the data subject and acknowledges that the Processor provides sufficient guarantees in this respect.

3.3 If required under local laws, Controller shall provide to the Processor a copy of the privacy notice that the Controller has delivered to the data subjects.

4 INSTRUCTIONS

4.1 Controller instructs Processor to process the personal data only on behalf of Controller. Controller's instructions are provided in this DPA and the Agreement. Controller is obliged to ensure that any instruction given to the Processor is in compliance with applicable data protection law. Processor is obliged to process the personal data only in accordance with the instructions given by the Controller unless otherwise required by European Union law, Member State law or other applicable data protection law (in the latter case clause 5.4 (b) applies).

4.2 Any further instructions that go beyond the instructions contained in this DPA or the Agreement must be within the subject matter of this DPA and the Agreement. If the implementation of such further instructions results in costs for Processor, Processor shall inform Controller about such costs with an explanation of the costs before implementing the instructions. Only after Controller's confirmation to bear such costs for the implementation of the instructions, Processor is required to implement such further instructions. Controller shall give further instructions generally in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by Controller in writing without delay.

4.3 Processor shall immediately inform Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection law and request the Controller to withdraw, amend or confirm the relevant instruction. Pending the decision of the Controller on the withdrawal, amendment or confirmation of the relevant instruction, Processor shall be entitled to suspend the implementation of the relevant instruction.

5 OBLIGATIONS OF PROCESSOR

5.1 The Processor and persons authorized by Processor to process the personal data on behalf of Controller, in particular Processor's employees as well as employees of any Subprocessors, shall have committed themselves to confidentiality or shall be under an appropriate statutory obligation of confidentiality. Processor may not process personal data for purposes different than those that derive from or are related to the performance of its obligations under this DPA, or for purposes different that those instructed by the Controller.

5.2 Processor is obliged to implement the technical and organizational measures as specified in Appendix 3 before processing the personal data on behalf of Controller. Processor may amend

the technical and organizational measures from time to time provided that the amended technical and organizational measures are not less protective as those set out in Appendix 3.

5.3 Processor is obliged to make available to Controller information in order to demonstrate compliance with the obligations of Processor laid down in Art. 28 GDPR. The Parties agree that this information obligation is met by providing Controller with an audit report upon request ("**Audit Report**"). To the extent additional audit activities are legally required, Controller may request inspections conducted by Controller or another auditor mandated by Controller ("**On-Site Audit**"). Such On-Site Audit is subject to the following conditions:

(a) On-Site Audits are limited to processing facilities and personnel of Processor involved in the processing activities covered by this DPA; and

(b) On-Site Audits occur not more than once annually or as required by applicable data protection law or by a competent supervisory authority or immediately subsequent to a material personal data breach that affected the personal data processed by Processor under this DPA; and

(c) may be performed during regular business hours, solely insubstantially disrupting the Processor's business operations and in accordance with Processor's security policies, and after a reasonable prior notice; and

(d) Controller shall bear any costs arising out of or in connection with the On-Site Audit at Controller and Processor.

Controller is obliged to create an audit report summarizing the findings and observations of the On-Site Audit ("**On-Site Audit Report**"). On-Site Audit Reports as well as Audit-Reports are confidential information of Processor and shall not be disclosed to third parties unless required by applicable data protection law or subject to Processor's consent.

5.4 Processor is obliged to notify Controller without undue delay:

(a) about any legally binding request for disclosure of the personal data by a law enforcement authority, unless otherwise prohibited, such as by a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(b) if Processor or Subprocessor is required pursuant to European Union law, Member State law or other applicable data protection law to which Processor or Subprocessor is subject to process the personal data beyond the instructions of Controller, before carrying out such processing beyond the instruction, unless that European Union law, Member State law or other applicable data protection law prohibits such information on important grounds of public interest, in which case the notification to Controller shall specify the legal requirement under such European Union law Member State law or other applicable data protection law; and/or

(c) after Processor has documented reason to believe that a personal data breach at Processor or its Subprocessors has occurred that may affect the personal data of Controller covered by this DPA. In this case, Processor will assist Controller with Controller's obligation under applicable data protection law to inform the data subjects and the supervisory authorities, as applicable, by providing information according to Art. 33 (3) GDPR or other applicable data protection law as available to Processor. Processor shall implement remediation measures and corrective measures in order to prevent further breaches to occur again.

5.5 Processor is obliged to assist Controller with its obligation to carry out a data protection impact assessment as may be required by Art. 35 GDPR or under any other applicable data protection

law and prior consultation as may be required by Art. 36 GDPR that relates to the Services provided by Processor to Controller under this DPA by means of providing the necessary and available information to Controller. Processor shall be obliged to provide such assistance only insofar that Controller's obligation can not be met by Controller through other means. Processor will advise Controller on the costs for such assistance. Once Controller has confirmed to bear such costs, Processor will provide such assistance.

5.6 Processor is obliged - at the choice of the Controller - to delete or return to Controller all the personal data (and data storage media, which had been handed over by Controller, if any) which are processed by Processor on behalf of Controller under this DPA after the end of the provision of Services, and delete any existing copies unless European Union, Member State law or other applicable local law requires Processor to retain such personal data.

6 DATA SUBJECT RIGHTS

6.1 Controller is primarily responsible for handling and responding to requests made by data subjects.

6.2 Processor is obliged to assist Controller with appropriate and possible technical and organizational measures to respond to requests for exercising the data subjects' rights which are laid down in Chapter III of the GDPR or other applicable data protection laws.

7 SUBPROCESSING

7.1 Controller authorizes the use of Subprocessors engaged by Processor for the provision of the Services under this DPA. The same applies to the use of further Subprocessors engaged by Subprocessors, in which case the below applies accordingly. Processor shall choose such Subprocessor diligently. Processor remains responsible for any acts or omissions of its Subprocessors in the same manner as for its own acts and omissions hereunder. Controller approves the following Subprocessors:

7.2

Name	Address	Purpose of use
Software AG	Uhlandstraße 12 64297 Darmstadt Germany	provision of Cloud Services

7.3 Processor shall pass in writing (electronic form is sufficient) to Subprocessors the obligations of Processor under this DPA to the extent applicable to the subcontracted Services.

7.4 Processor may remove, replace or appoint suitable and reliable further Subprocessors at its own discretion in accordance with this clause:

(a) Processor shall notify Controller in advance of any changes to the list of Subprocessors as set out under clause 7.1. If Controller does not object in accordance with this clause 7.3 (b) within thirty days after receipt of Processor’s notice the further Subprocessor(s) shall be deemed accepted.

(b) If Controller has a legitimate reason to object to a Subprocessor, Controller shall notify Processor thereof in writing within thirty days after receipt of Processor's notice. If Controller objects to the use of the Subprocessor, Processor shall have the right to cure the objection within thirty days after Processor's receipt of Controller's objection If the

objection has not been cured within thirty days after Processor's receipt of Controller's objection, either party may terminate the affected Service with reasonable prior written notice.

7.5 This clause shall not apply to Controllers based in Israel.

8 LIMITATION OF LIABILITY

8.1 Any liability arising out of or in connection with a violation of the obligations of this DPA or under applicable data protection law, shall follow, and be governed by, the liability provisions set forth in, or otherwise applicable to, the Agreement, unless otherwise provided within this DPA.

9 INDEMNITY

9.1 The Controller shall defend, indemnify, and hold harmless Processor and the officers, directors, employees, successors, and agents of Processor (collectively, “indemnified parties”) from all claims, damages, liabilities, assessments, losses, costs, administrative fines and other expenses (including, without limitation, reasonable attorneys' fees and legal expenses) arising out of or resulting from any claim, allegation, demand, suit, action, order or any other proceeding by a third party (including supervisory authorities) that arises out of or relates to the violation of Controller's obligations under this DPA and/or applicable data protection law.

10 DURATION AND TERMINATION

10.1 The term of this DPA is identical with the term of the Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Agreement.

11 GENERAL

11.1 In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this DPA shall prevail.

11.2 If any provision of this DPA is held to be invalid, illegal or unenforceable, the remaining provisions shall not be affected or impaired.

11.3 This DPA shall be governed by the same law as the Agreement.

Agreement			
Duly authorized for and on behalf of Processor acting in its own name and acting in the name and on behalf of the processors listed in Appendix 4 (each a "**Processor**")		Duly authorized for and on behalf of Controller	
Signed	stan.smith@softwareag.com Digitally signed by stan.smith@softwareag.com DN: cn=stan.smith@softwareag.com Date: 2018.05.22 11:32:22 -04'00'	Signed	
Name	Stan Smith	Name	
Title	SVP, General Counsel	Title	
Date		Date	

APPENDIX 1

STANDARD CONTRACTUAL CLAUSES

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

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.

2 Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 2 which forms an integral part of the Clauses.

3 Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

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

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

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 Appendix 3 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 Appendix 3, and a summary description of the security measures, as well as a copy of any contract for subprocessing 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 subprocessing, 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).

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 Appendix 3 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 subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 3 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 subprocessing, 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.

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 of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

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.

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).

9 Governing Law

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

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.

11 Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the 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 subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing 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.

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.

APPENDIX 2

DETAILS OF PROCESSING

Controller/Data Exporter

The Controller/Data Exporter performs the following activities relevant to the transfer (Controller to specify):

- The Controller/Data Exporter is providing business data necessary in course of use of and to assist in the analysis and resolution of Support Incidents reported in the Cloud Services of Processor/Data Importer

Processor/Data Importer

The Processor/Data Importer is a member of the Software AG group.

Data subjects

The personal data transferred concern the following categories of data subjects (Controller to specify):

- employees of Controller/Data Exporter
- potentially end customers of the Controller/Data Exporter

Categories of data

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

- Name
- Corporate Personnel ID
- Business e-mail address
- Telephone number
- IP Address
- Payment Terms

Special categories of data (if appropriate)

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

- The transfer of special categories of personal data is not anticipated.
- The Controller/Data Exporter decides which data is transmitted for the purpose of providing Cloud Services

Processing operations

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

- Processor/Data Importer processes Controller/Data Exporter Data with a Software as a Service /Platform as a Service in a public cloud infrastructure as defined in the Cloud Services agreement

Subject matter of the processing

The subject matter of the data processing under this addendum is the Controller/Data Exporter data processed in the cloud services as defined in the Cloud Services Attachment including the operation of a

Cloud Service platform. To access the operated platform users need to be authenticated and authorized. User details will be used to create unique user id's that are used for authentication and authorization. Email addresses might be used to send notifications to the users as result of using services of the Cloud Service platform and corresponding support systems (e.g. Ticket system).

Nature and purpose of the processing

Processor/Data Importer processes the personal data of the data subjects on behalf of Controller/Data Exporter in connection with the following:

- The purpose of the data processing under this addendum the provisioning of the Cloud Services initiated by the Controller/Data Exporter. The Cloud Services processing systems and respective processing properties are defined in the Cloud Services Attachment

APPENDIX 3

TECHNICAL AND ORGANIZATIONAL 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 risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor/Data Importer shall implement the following technical and organizational measures which have been confirmed as appropriate by the Controller/Data Exporter to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons. In assessing the appropriate level of security Controller/Data Exporter took account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

A. GENERAL TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

As of the Data Processing Agreement Effective Date Processor/Data Importer's entity set out in the relevant Cloud Services Attachment as the entity delivering the Cloud Services (hereinafter "**Cloud Service Unit**" or "**CSU**") is verified under ISO/IEC 27001 and agrees to maintain an information security program for the services that complies with the ISO/IEC 27001 standards or such other alternative standards as are substantially equivalent to ISO/IEC 27001 for the establishment, implementation, control and improvement of the Cloud Service Unit Security Standards.

1 CONFIDENTIALITY (ART 32 PARA. 1 LIT B GDPR)

1.1 **Access Control of Processing Areas**: Processor/Data Importer shall implement suitable measures to prevent unauthorized persons from gaining access to the data processing equipment where the personal data is processed. This is accomplished through the following measures:

(a) Processor/Data Importer facilities access is strictly controlled. Physical access to sensitive IT facilities is regulated via Processor/Data Importer's Physical Access Policy.

(b) Cloud Service Unit (CSU)'s Infrastructure as a Service sub-processor (IaaS Supplier), identified in the Cloud Services Attachment, maintains physical access control over the Cloud Services data processing equipment. The respective physical security mechanisms of the IaaS Supplier are reviewed by independent external audits in regards to ISO/IEC 27001 compliance.

1.2 **Access Control to Data Processing Systems**: Processor/Data Importer shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished through the following measures:

(a) The following will be applied, among other controls, depending upon the particular Cloud Services subscribed: authentication via passwords and/or multi-factor authentication, documented authorization processes, documented change management processes and logging of access on several levels.

(b) Access to Controller/Data Exporter data and systems is controlled in accordance with

CSU's Access Control Policy aligned with the ISO/IEC 27001 Standard (Refer to Annex A 9 for additional details).

1.3 **Access Control to Use Specific Areas of Data Processing Systems**: Processor/Data Importer shall commit that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied, modified, or removed without authorization. This is accomplished through the following measures:

(a) Operational System Administrative access is granted based on the principle of least privilege. Access controls to be applied include a documented change management process and the use of multi-factor authentication and encryption. This access is controlled in alignment with CSU's Access Control Policy, Clear Desk and Clear Screen Policy, Cryptographic Controls Policy and Data Privacy Policy.

(b) Data transfer requirements of the CSU's Communication Security Policy are aligned with the ISO/IEC 27001 Standard (Refer to Annex A 13 for additional details).

(c) Backup up of Controller/Data Exporter tenant data and protection of log files are controlled in alignment with the ISO/IEC 27001 Standard (Refer to Annex A 12 for additional details).

1.4 **Separation of Processing for Different Purposes**: Processor/Data Importer shall implement suitable measures to make sure that data collected for different purposes can be processed separately. This is accomplished through the following measures:

(a) Processing of tenant content is directly encapsulated in the cloud application accessed via the cloud service. Access control to the tenant application is in the responsibility of the Controller/Data Exporter. All Controller/Data Exporter tenant content is directly encapsulated in the logically segregated tenant database.

1.5 **Pseudonymization**: In order to achieve the purposes of the commissioned data processing it is not possible to pseudonymize the Personal Data.

1.6 **Encryption**: Encryption of Controller/Data Exporter data at rest and in transit is ensured and controlled by the CSU's Cryptographic Controls Policy aligned with the ISO/IEC 27001 Standard (Refer to Annex A 10 for additional details).

2 INTEGRITY (ART 32 PARA. 1 LIT B GDPR)

2.1 **Input control**: Processor/Data Importer shall implement suitable measures to make sure that it can check and establish whether and by whom personal data has been inputted into data processing systems or removed. This is accomplished through the following measures:

(a) The source of Personal Data is under the control of the Controller/Data Exporter, and Personal Data input into the system, is managed by secured file transfer (i.e., via web services or entered into the application) from the Controller/Data Exporter. Note - specific Cloud Services may permit Controllers/Data Exporters to use unencrypted file transfer protocols, in such cases, Controller/Data Exporter is solely responsible for its decision to use such unencrypted field transfer protocols.

(b) Only authorized personnel will be able to access the production cloud infrastructure of Controller/Data Exporter data processing for the sole purpose of management and maintenance functions. All personnel have a unique user-id and use strong passwords according to CSU's Login and Password Policy and all such activities are monitored and logged.

2.2 **Transmission Control**: Processor/Data Importer implements suitable measures to prevent the

personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished through the following measures:

(a) For all production cloud environments IaaS provider security mechanisms are used to provide private, isolated areas for Processor/Data Importer Cloud where respective Cloud resources are launched in a defined virtual network. All scoped data is stored in a virtual cloud environment and is transmitted through HTTPS with up-to-date encryption ciphers.

(b) Controller/Data Exporter tenant Data-at-rest for Cloud Services are encrypted. Except as otherwise specified for the Cloud Services (including within the ordering document or the applicable service specifications), transfers of data outside the Cloud Service environment are encrypted. The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted. Controller/Data Exporter is solely responsible for the results of its decision to use unencrypted communications or transmissions.

(c) Data transfer requirements of the CSU's Communication Security Policy protect the transfer of Controller/Data Exporter tenant data through the use of all types of communication facilities.

3 AVAILABILITY AND RESILIENCE (ART 32 PARA. 1 LIT B GDPR)

3.1 **Availability Control**: Processor/Data Importer shall implement suitable measures to make sure that personal data is protected from accidental destruction or loss. This is accomplished through the following measures:

(a) Any changes to the production environments are fully monitored. CSU performs regular tenant backups to be able to restore virtual machine images and tenant data according to the Recovery Point Objectives and Recovery Time Objectives specified in the relevant Cloud Services Attachment.

(b) Control of availability for Cloud Services is ensured under CSU's Information Security Continuity Management and Operations Backup and Restore Controls aligned with the ISO/IEC 27001 Standard (Refer to Annex A 12 and 17 for additional details).

(c) The CSU's IaaS Supplier services are protected from utility service outages in alignment with the ISO/IEC 27001 standard as validated and certified by an independent auditor. procedures, and the identification of the person who carried them out.

3.2 **Resilience**: External access to all cloud production networks and systems is protected by Firewalls and Intrusion Detection Prevention Systems used to limit/filter network traffic. Cloud Services Disaster recovery is tested and reviewed on a yearly basis.

4 PROCESS FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANIZATIONAL MEASURES FOR ENSURING THE SECURITY OF THE DATA PROCESSING (ART. 32 PARA. 1 LIT. D GDPR)

4.1 **Data protection management**: In addition to the access control rules set forth in Sections Access control of processing areas and Access control to data processing systems, Controller/Data Exporter controls access to its Cloud Services and to Personal Data and other data through its authorized personnel. Personal Data from different Controllers/Data Exporters' environments are logically segregated. CSU's policy does not allow the replication of

Controller/Data Exporter's production data to non-production environments unless explicitly requested by Controller/Data Exporter.

4.2 **Incident Response Management**: CSU has implemented a Security Incident Response Process and Security Incident Response Policy aligned with the ISO/IEC 27001 Standard (Refer to Annex A 16 for additional details). Controllers/Data Exporters are made aware of their responsibilities in the context of Cloud Service and Cloud Support Agreements. Security Incidents are tracked with the Processor/Data Importer incident management tool. Controller/Data Exporter point of contacts are notified via e-mail according to the Security Incident Response Policy. The incident response program of the IaaS Supplier (detection, investigation and response to incidents) has been developed in alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored.

4.3 **Data Protection by default (Art. 25 para. 2 GDPR)**: CSU has data protection policies and controls in place which prohibit CSU staff from accessing tenant data unless explicitly authorized and granted by the Controller/Data Exporter tenant administrator. All Controller/Data Exporter tenant content is directly encapsulated in the logically segregated tenant database. Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced. Default configurations of Cloud Services are designed to process only Personal Data required to deliver the service.

4.4 **Job Control**: Processor/Data Importer implements suitable measures to ensure that the personal data is processed in accordance with the instructions of the Controller. This is accomplished through the following measures:

(a) The control of Personal Data remains with Controller/Data Exporter, and as between Controller/Data Exporter and CSU, Controller/Data Exporter will at all times remain the Controller for the purposes of the Cloud Services, the Cloud Services Agreement, and the Data Processing Agreement. Controller/Data Exporter is responsible for compliance with its obligations as Controller under data protection laws, in particular for justification of any transmission of Personal Data to CSU (including providing any required notices and obtaining any required consents), and for its decisions and actions concerning the Processing and use of the data.

(b) CSU will process Personal Data solely for the provision of the Cloud Services, and will not otherwise (i) process or use Personal Data for purposes other than those set forth in the Cloud Services Agreement or as instructed by Controller/Data Exporter, or (ii) disclose such Personal Data to third parties other than CSU Cloud Operations supporting units or Subprocessors for the aforementioned purposes or as required by law.

(c) Access to Controller/Data Exporter data and systems are controlled in accordance with CSU's Access Control Policy and Operations Security Controls aligned with the ISO 27001 Standard (Refer to Annex A 9 and 12 for additional details).

4.5 **Job Control – Owners and Engineers**: Processor/Data Importer shall further implement suitable measures to monitor its cloud service system system administrators and to ensure that they act in accordance with instructions received. This is accomplished through the following measures:

(a) Individual appointment of system administrators;

(b) Adoption of suitable measures to log system administrators' access and keep those logs secure, accurate and unmodified for at least six months;

(c) Yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by importer and applicable laws; and

(d) Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned.

B. ADDITIONAL COUNTRY SPECIFIC MEASURES

The following additional country specific measures apply to Controllers based in the countries listed below:

Australia:

The following amendments apply only in respect of the processing of personal data by the Processor on behalf of a Controller which has an Australian link in respect of that personal data within the meaning of the Privacy Act 1988 (Cth) ("**Australian Data**"), irrespective of whether the country where the Data Importer is located has been designated by the European Commission as ensuring an adequate level of protection pursuant to Article 25(6) of the Data Protection Directive or from May 25, 2018 within the meaning of Article 45 (1) General Data Protection Regulation:

1 In this DPA, references to

(a) a "Member State" includes Australia;

(b) the "General Data Protection Regulation", "GDPR", "Directive 95/46/EC", "applicable data protection laws" ("EU Privacy Laws"), and any provisions, sections, Chapters or Articles of those of those EU Privacy Laws, in the Agreement shall be replaced with the term "Privacy Act 1988 (Cth) and any applicable state and territory-based privacy laws, and all related laws and regulations" ("Australian Privacy Laws");

(c) "personal data" shall be read as including personal information within the meaning of Australian Privacy Laws;

(d) the "supervisory authority" shall be read as references to the competent regulatory authority pursuant to Australian Privacy Laws; and

(e) "special categories of data" and "sensitive data" shall be read as including sensitive information within the meaning of Australian Privacy Laws;

2 The Processor will take reasonable steps to protect Australian Data it processes from misuse, interference and loss and from unauthorized access, modification or disclosure;

3 The Processor will notify the Controller without undue delay of: (i) any known or reasonable ground to believe of non-compliance with statutory provisions dealing with the protection of Australian Data by the Processor or its employees, and (ii) any known or reasonable ground to believe of non-compliance with the provisions of this DPA. The Processor shall further notify the Controller, without undue delay, if it holds that an instruction violates applicable laws. Upon providing such notification, the Processor shall not be obliged to follow the instruction, unless and until the Controller has confirmed or changed it. The Processor shall notify the Controller of data subjects' complaints and requests (e.g., regarding the rectification, deletion and blocking of data) and orders by courts and competent regulators and any other exposures or threats in relation to data protection compliance identified by the Processor and shall provide reasonable assistance to the Controller to respond to such complaints or requests in a timely manner. Notwithstanding (i) and (ii) above, the Processor will provide the Controller immediately with a data breach notice if the Processor has reasonable grounds to believe there has been any security incident that is

likely to have impact on the availability, integrity and / or confidentiality of the Australian Data processed by the Processor (e.g., discovery of unintended data deletion, discovery of data being accessible to resources that were not or no longer authorized, discovery of unintended disclosure or data potentially having become compromised by a hacking attack or other external security threat). The data breach notice must contain as a minimum the scope of the Australia Data affected, the scope and number of data subjects affected, the time when the data breach took place, the circumstances, and the effects of the data breach, and the measures taken to eliminate the consequences of the breach and further information the Controller may require to comply with Australian Privacy Laws;

4 Australian Data must be destroyed or permanently de-identified after it is no longer required for a purpose permitted by this DPA. The Processor must obtain written confirmation from the Controller that Australian Data is no longer required prior to destroying or de-identifying that Australian Data.

5 Australian Data may only be processed for direct marketing where the data subject has expressly consented to such processing, or as otherwise agreed by the Controller in writing;

6 Identifiers of data subjects that have been assigned by or on behalf of any Australian government organisation must not be used or disclosed unless required or authorised by Australian law; and

7 Sensitive data may only be processed as authorised by the data subject, unless the Controller otherwise agrees in writing.

Belgium:

1 It is agreed that each Processor subscribes this DPA for its own purposes and its own data processing, without being bound jointly or severally (“solidairement ou indivisiblement”) with the others.

2 By express deviation from Article 1325 of the Belgian Civil Code, this DPA may be validly executed separately by each signatory and shall be properly evidenced by the production of any original or non original copy thereof together with the signature pages (or copies thereof) of the other relevant parties. The Parties waive any and all evidentiary and/or other requirements as to the execution of this DPA other than those enunciated in this section for Belgium.

India:

1 The Processor shall ensure the same or greater level of data protection, as is adhered to by the Controller, under the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Israel:

1 The Processor/Data Importer will provide a report to the Controller, at least once a year, with respect to the manner in which it performs its duties under the Israeli Information Security Regulations and this DPA and will notify the Controller of the occurrence of any security event in which the personal data is involved.

2 The Processor/Data Importer undertakes that it will and will procure the authorized persons on its

behalf will maintain all the necessary security measures required in accordance with any applicable law in connection with the personal data, including any requirement for the protection of the integrity of such personal data and protection against any unlawful disclosure, use or copy thereof.

3 The Processor/Data Importer undertakes to provide the Controller, upon its reasonable demand, reports concerning the security measures implemented by it and will allow the Controller and/or anyone acting on its behalf.

4 The Processor/Data Importer undertakes to provide from time to time and in any event no less than once a year tutorials to anyone acting on its behalf in connection with the obligations under this DPA, including the duty to maintain the personal data in strict confidence.

5 The Processor/Data Importer will comply with all requirements of the Controller regarding data security which are required under applicable data protection laws as shall be informed to the Processor/Data Importer from time to time, The Processor Data Importer shall limit or prevent the possibility of connecting portable devices to the systems in which the personal data is stored.

6 The Processor/Data Importer shall ensure that ongoing updates are performed on the database systems in which the personal data is stored.

7 When applicable according to the Israeli Information Security Regulations, the Processor/Data Importer should take measures to control and document the entry into, and exit from, the locations where the systems in which the personal data is processed are situated and of the introduction and removal of equipment into and from such sites.

8 The Processor/Data Importer shall grant permission to access to the personal data or change its scope after reasonable measures are taken by it. Access permissions to the personal data will be determined according to job definitions.

9 Processor/Data Importer shall commit that the persons entitled to use its data processing system should sign applicable confidentiality undertakings according to which they will keep the information confidential and that they will use the information only for the purposes of providing the Services to the Data Exporter.

10 Processor/Data Importer shall implement suitable measures to make sure that it can check and establish when there was access to the personal data.

11 Processor/Data Importer shall revoke the authorizations of an authorized person that has finished his role. and, insofar as possible, immediately upon termination of the authorized person’s role, change the passwords that the authorized person might have known.

12 The systems in which the personal data is stored shall not be connected to the internet or to any other public network without the installation of appropriate means of protection from unauthorized intrusion, or from programs capable of causing damage or disruption to the computer or computer material (including the use of accepted means of encryption). In relation to a system that can be accessed remotely using the internet or another public network, security measures additional to those set forth shall be taken whose objective is to identify the party making the connection and to verify his authorization to perform the operations remotely and its scope.

Luxembourg:

1 It is agreed that each Processor subscribes this DPA for its own purposes and its own data processing, without being bound jointly or severally (“solidairement ou indivisiblement”) with the others.

2 Done in [two] originals, each Party acknowledgement receipt of one duly signed original.

Malaysia:

1 Processor / Data Importer shall adopt the following security measures in accordance with the requirements of the Personal Data Protection Standard 2015:

(a) to maintain a register of all its employees involved in the processing of personal data;

(b) discontinue its employees' rights after the end of service, termination, and end of contractual / agreement term, or pursuant to organizational changes;

(c) control and limit the extent of its employees' right to access personal data;

(d) control the outward and inward movement in respect of data storage locations;

(e) update all back up / recovery systems and anti-virus software to protect personal data from incidents of invasion;

(f) protect computer systems from malware threats against personal data;

(g) to ensure that the transfer of personal data through removable media device and cloud computing service is only with the written authorization of senior management of the processor;

(h) to record all transfer of personal data which utilizes a removable media device and cloud computing service; and

(i) to maintain an accurate periodic personal data access record and to disclose the records when requested by the Malaysian Personal Data Protection Department.

Mexico:

1 Processor/Data Importer shall define the functions and obligations applicable to officers in charge of the protection of the personal data;

2 Data Importer shall implement a suitable data protection management in its organization, including those set out below:

(a) Create and maintain inventories of: (i) personal data items collected from data subjects and; (ii) security systems and storage infrastructure used for the processing the personal data;

(b) Conduct security measures gap analysis and carry out regular security risks audits and assessments to identify and evaluate possible risks and areas of improvement;

(c) Design and implement action plans to address any issues identified in such assessments and audits;

(d) Provide appropriate training to staff involved in the data processing activities;

(e) Update Security Measures accordingly to improve such measures either as result of recommendations derived from audits or assessments or after the confirmation of any unauthorized access or disclosure of personal data.

APPENDIX 4

LIST OF PROCESSORS

#	Country	Name	Address	Data Processing Operation
1	Australia	Software AG Cloud APJ PTY Ltd.	Level 16, 201 Miller Street North Sydney, NSW 2060	Cloud Services and Support
2	Brazil	Software AG Brasil Informatica e Serviços Ltda	Av. das Nações Unidas 12.901, 33° andar, Torre Norte CEP 04578-000 São Paulo/SP	Cloud Services and Support
3	India	Software AG Chennai Development Center India Pvt Ltd	VBC Solitaire, 4th Floor, No. 47 & 49, Bazulla Road, T. Nagar 600 017 Chennai	Cloud Services and Support
4	India	Software AG Bangalore Technologies Private Ltd.	Embassy Tech Village 5th and 6th Floor, 2A East Tower, Marathahalli Outer Ring Road 560 103 Devarabisanahalli Bangalore	Cloud Services and Support
5	Japan	Software AG Ltd. Japan	AKASAKA K-Tower 4F, 1-2-7 Motoakasaka 107-0051 Minato-ku, Tokyo	Cloud Services and Support
6	Malaysia	Software AG Operations Malaysia Sdn Bhd.	Suite 2B-22-1, Level 22, Block 2B, Plaza Sentral, Jalan Stesen Sentral 5, Kuala Lumpur Sentral, 50470 Kuala Lumpur	Cloud Services and Support
7	Mexico	Software AG, S.A. de C.V.	Blvd Manuel Avila Camacho No. 88 Piso 11, Torre Picasso, Col. Lomas de Chapultepec 11590 Mexico, Distrito Federal	Cloud Services and Support
8	USA	Software AG Cloud Americas, Inc.	1209 Orange Street Wilmington , DE 19801	Cloud Services and Support

The following additional country specific measures apply to Controllers based in Israel:

#	Country	Name	Address	Data Processing Operation
1	Australia	Software AG Cloud APJ PTY Ltd.	Level 16, 201 Miller Street North Sydney, NSW 2060	Cloud Services and Support
2	Belgium	Software AG Belgium S.A.	Chaussée de la Hulpe, 166 1170 Watermael-Boitsfort	Cloud Services and Support
3	Bulgaria	Software AG Development Center Bulgaria EOOD	115L Tsarigradsko shose Blvd., Business building C, fl. 3 1784 Sofia	Cloud Services and Support
4	Brazil	Software AG Brasil Informatica e Serviços Ltda	Av. das Nações Unidas 12.901, 33° andar, Torre Norte CEP 04578-000 São Paulo/SP	Cloud Services and Support
5	Canada	Software AG Inc.	231 Shearson Crescent, Suite 101 N1T1J5 Cambridge, Ontario	Cloud Services and Support
6	France	Software AG France SAS	20, Avenue André Prothin, Tour Europlaza La Défense 4 92927 Paris La Défense Cedex	Cloud Services and Support
7	Germany	Cumulocity GmbH	Speditionsstraße 13 40221 Düsseldorf	Cloud Services and Support
8	Germany	SAG Cloud GmbH	Uhlandstr. 12 64297 Darmstadt	Cloud Services and Support
9	Germany	Software AG	Uhlandstr. 12 64297 Darmstadt	Cloud Services and Support
10	India	Software AG Chennai Development Center India Pvt	VBC Solitaire, 4th Floor, No. 47 & 49, Bazulla Road, T. Nagar	Cloud Services and Support

		Ltd	600 017 Chennai	
11	India	Software AG Bangalore Technologies Private Ltd.	Embassy Tech Village 5th and 6th Floor, 2A East Tower, Marathahalli Outer Ring Road 560 103 Devarabisanahalli Bangalore	Cloud Services and Support
12	Israel	S.P.L. Software Ltd.	3B Yoni Netanyahu Street 6037602 OR-Yehuda	Cloud Services and Support
13	Japan	Software AG Ltd. Japan	AKASAKA K-Tower 4F, 1-2-7 Motoakasaka 107-0051 Minato-ku, Tokyo	Cloud Services and Support
14	Malaysia	Software AG Operations Malaysia Sdn Bhd.	Suite 2B-22-1, Level 22, Block 2B, Plaza Sentral, Jalan Stesen Sentral 5, Kuala Lumpur Sentral, 50470 Kuala Lumpur	Cloud Services and Support
15	Mexico	Software AG, S.A. de C.V.	Blvd Manuel Avila Camacho No. 88 Piso 11, Torre Picasso, Col. Lomas de Chapultepec 11590 Mexico, Distrito Federal	Cloud Services and Support
16	Netherlands	Software AG Nederland B.V.	Loire 162 2491 IL Den Haag	Cloud Services and Support
17	Poland	Software AG Polska Sp. z o.o.	ul. Piêkna 18 00-549 Warszawa	Cloud Services and Support
18	Slovakia	Software AG Development Centre Slovakia s.r.o.	Južna trieda 125 04001, C.R. Košice	Cloud Services and Support
19	Spain	Software AG ESPAÑA, S.A. Unipersonal	Ronda de la Luna, 22 E-28760 Tres Cantos, Madrid	Cloud Services and Support

20	United Kingdom	Software AG (UK) Limited	Locomotive Way GB - DE24 8PU Derby	Cloud Services and Support
21	USA	Software AG Cloud Americas, Inc.	1209 Orange Street Wilmington, DE 19801	Cloud Services and Support
22	USA	Software AG USA, Inc.	11700 Plaza America Drive, Suite 700 Reston, VA 20190	Cloud Services and Support