HOW TO EXECUTE THIS DPA:

To complete this DPA, Customer must:
• Click on the link here: https://ironcladapp.com/public-launch/6516ae409104c08dc8f041ac.
• Fill in the form with your details, please indicate also the Product Tier or Agreement that you are subscribed to and the Use Case.
• The Countersigned copy will automatically be sent to the e-mail provided in the form.

VARIABLES		
Parties' relationship	Controller (Counterparty) and Processor (Camunda)	
Parties' roles	Counterparty will act as the Controller and Business (as defined in Section 1 of the Terms) Camunda will act as the Processor (as defined in Section 1 of the Terms)	
Contacts	Counterparty	Camunda
	Name: Email:	Name: Camunda (Entity) Email: privacy@camunda.com
Main Agreement	Insert	
Term	This DPA will commence on the final date of signature and will continue per the main agreement	
Breach Notification Period	Without undue delay after becoming aware of a personal data breach	
Sub-processor Notification Period	14 days before the new sub-processor is granted access to Personal Data	

Liability Cap	The liability caps as per the Main Agreement
Governing Law and Jurisdiction	As per the Main Agreement
Data Protection Laws	All laws, regulations and court orders which apply to the processing of Personal Data in: • Insert Data Protection Laws • This includes the European Union Regulation (EU) 2016/679, the Data Protection Act 2018[endif], California Consumer Privacy Act of 2018 (**CCPA**)/California Privacy Rights Act of 2020 (**CPRA**), as amended from time to time.
Services related to processing	As described in the Main Agreement
Duration of processing	As per the Main Agreement
Nature and purpose of processing	The nature and purpose of the data processing under this DPA is the provision of the Services and providing the Software and/or the Services to Customer and the performance of Camunda's obligations under the Agreement and this DPA (or as otherwise agreed by the Parties.
Personal Data	The types of personal data processed are (Insert types of personal data)
Data subjects	The individuals whose Personal Data will be processed are (Insert data subject)
Special provisions	(For US) In this DPA, where California Law applies, (1) references to the Controller and corresponding provisions and obligations will be construed as references to a Business within the meaning of CCPA/CPRA, and (2) references to the Processor and corresponding provisions and obligations will be construed as references to a Service Provider within the meaning of CCPA/CPRA. (For EEA) If the Controller is located outside the EEA, enters into this DPA with Camunda Services GmbH as a Processor, and chooses a data location within the EEA, the parties hereby agree that Module 4) of the SCC (Controller to Processor) apply and Camunda Services GmbH shall be acting a Data Exporter and Controller acting as Data Importer within the meaning of the SCC.

Transfer Mechanism	Standard Contractual Clauses approved by the European Commission Decision of 4 June 2021 (as amended from time to time), for the transfer of personal data from the EEA or adequate country to a third country.

ANNEX 1

Security measures. Technical and organisational measures to ensure the security of Personal Data	**Technical and Organizational Measures** **1. Pseudonymization (Art.32 para. 1 lit. a) GDPR; Art. 25 para. 1 GDPR)** (Measures suited to ensure the Personal Service Data cannot be associated with a specific Data Subject without the assistance of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures): • For support tickets no Personal Service Data is required by Camunda; Customer may pseudonymize Personal Service Data before sending it to the support team. **2) Confidentiality, Integrity, Availability and Resilience (Art. 32 para. 1 lit. a) GDPR; Art. 25 para. 1 GDPR)** a. Confidentiality (Art. 32 para. 1 lit. b) GDPR) Physical Access Control (Measures to prevent unauthorized access to data processing equipment with which Personal Service Data may be processed and used which GCP and AWS implement): • No unauthorized access to Personal Service Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems. • An effective and documented procedure exists to assign, alter, and withdraw access rights, incl. the return of the means of access. • Visitors in security zones are accompanied by authorized staff. • Data related to support inquiries are stored by Salesforce.com Germany GmbH in Germany (EU). • Camunda SaaS Enterprise is hosted at an external cloud service provider (currently Google Cloud Platform), with whom Camunda has a data processing agreement in place. Electronic Access Control (Measures to prevent unauthorized use of data processing systems): • Access is secured via a firewall, with strong encryption and by two-factor authentication mechanisms. • Secure passwords are used, and system and application default passwords are changed as a matter of principle. Their structure and handling are in accordance with a documented password guideline.

- An effective and documented access control policy exists.
- The access control policy is assessed at least once per year.
- All staff are instructed to lock their electronic workplaces specifically their laptops, by ensuring they are closed when left unattended. All company-provided laptops are configured with an automatic locking feature that activates when the device is idle.
- The access control policy defines the issuance and withdrawal of access rights, as well as their approval for internal and external staff.

Internal Access Control (Measures ensuring that authorized persons only have access to the Personal Service Data covered by their access authorization and that prevent unauthorized reading, alteration, or erasure during processing, use, and storage):

- Release of Personal Service Data only to authorized persons, including allocation of differentiated access rights and roles.
- Access rights are adjusted if the tasks carried out in the business processes change and/or are withdrawn if they are no longer needed

b. Integrity (Art. 32 para. 1 lit. b) GDPR)

Data Transfer Control (Measures that prevent unauthorized reading, alteration or erasure during processing, use and storage of Personal Service Data during electronic transfer, storage on data media or during transportation):

- Use of adequate encryption technologies
- No physical transport of the Personal Service Data (e.g. via data carriers)
- Use of adequate firewall, VPN, or other encryption technologies to protect the gateways and pipelines through which the Personal Service Data travels.

Data Entry Control (Measures that are suited to verify whether any by whom Personal Service Data has been entered into, altered in, or removed from data processing systems):

- Plausibility is guaranteed via the Login functions of the Camunda SaaS Enterprise.
- Log systems and logging information are protected against unauthorized access, alteration, and erasure, and are regularly evaluated.
- The clocks of all critical systems are synchronized using a reliable, agreed-time server.

Order Control (Measures that are suited for ensuring that the commissioned processing of personal data complies with the guidelines of the contracting Party):

- Camunda has data processing agreements with the sub-processors who process Personal Service Data on Camunda’s behalf in place.
- External service providers are evaluated before being contracted.

Separation rule (Measures that are suited for ensuring that data that has been collected for different purposes can be kept separate during processing):

- Access to Personal Service Data is separated through application security for the relevant Customers.
- Logical separation of Personal Service Data is implemented by using software controls to segregate data, such as different databases or separate access permission
- Development, testing, and production environments are separated.

c. Availability and Resilience (Art. 32 para. 1 lit. b) GDPR) (Measures to prevent accidental or willful destruction or loss):

- Camunda relies on its Cloud Service Providers for the redundancy of the physical infrastructure.
- Camunda ensures its Support infrastructure is backed up to a highly-available remote location.
- All Personal Service Data processed by Camunda SaaS Enterprise is stored on servers from our Cloud Service Provider
- High availability via redundant servers can be determined by Customer.

Incident-response-management (Measures suited to ensure that data breaches are recognised and reported quickly):

- A process has been established which ensures that security incidents are identified, assessed and dealt with appropriately.
- Escalation procedures and organisational interfaces are defined with all relevant parties, including the data protection officer.
- Staff who are responsible for the management of IT systems/applications are trained to recognise, classify and report security incidents.
- A process has been established which ensures information security for all critical business processes, even during a crisis or catastrophe.
- Processes and responsibilities have been defined in case of an emergency or crisis, and appropriate tests are held

d. Regular testing, assessment and evaluation processes (Art. 32 Paragraph 1 Point d) GDPR) (Measures guaranteeing that the data protection requirements are implemented):

- Relevant staff are trained and familiarised with data protection and placed under an appropriate obligation.
- The IT operation procedures (e.g. user management, backup, network management) are comprehensibly documented, regularly checked and altered where necessary.
- Identification, provision and testing of updates are a part of standard operation.

	• Regulations exist for information security and data protection. • The regulations for information security and data protection, as well as the security measures, are tested regularly for compliance and effectiveness.

ANNEX 2			
Sub-processors.		Overview Below	
Sub-processor	**Registered Address**	**Purpose**	**Processing Location**
Camunda, Inc.	**1209 Orange Street** **Wilmington, DE 19801** **United States**	**Support & maintenance in follow** **the sun model**	**USA**
Camunda Ltd	**Moorcrofts Llp** **Thames House** **Mere Park,** **Dedmere Road** **Marlow, SL7 1PB,** **United Kingdom**	**Support & maintenance in follow** **the sun model**	**United Kingdom**
Camunda Services GmbH	**Zossener Str. 55-58,** **10961 Berlin**	**Support & maintenance in follow** **the sun model**	**Germany**
Camunda PTE Limited	**16 Raffles Quay, #33-03** **Hong Leong Building** **Singapore 048581**	**Support & maintenance in follow** **the sun model**	**Singapore**

Cloudflare, Inc.	**Cloudflare, Inc.** **101 Townsend St** **San Francisco** **CA 94107** **United States**	**Application Firewall for Camunda Platform SaaS**	**Worldwide (depending on Customer's location)**
Google Cloud EMEA Limited	**70 Sir John Rogerson's Quay, Dublin 2,** **Ireland**	**Camunda SaaS Enterprise Infrastructure**	**Depending on customer setup, offering of Camunda and used services as described here: https://docs.camunda.io/docs/reference/regions/**
Amazon Web Services EMEA SARL	**38 Avenue John F. Kennedy, Luxembourg 1855, Luxembourg**	**Camunda SaaS Enterprise Infrastructure**	**Depending on customer setup, offering of Camunda and used services as described here: https://docs.camunda.io/docs/reference/regions/**
Salesforce.com Germany GmbH	**Erika-Mann-Str. 31 80636 München Germany**	**Customer Support Platform**	**Data Hosting Location: Germany**

TERMS

What is this agreement about?

1. **Purpose**. The parties are entering into this Data Processing Agreement (**DPA**) for the purpose of processing Personal Data (as defined above).
2. **Definitions.** Under this DPA:
    i. **adequate country** means a country or territory that is recognised under Data Protection Laws from time to time as providing adequate protection for processing Personal Data,
    ii. **Controller**, **data subject**, **personal data breach**, **process/processing,Processor** and **supervisory authority** have the same meanings as in the Data Protection Laws,
    iii. **(FOR USA) Business** and **Service Provider** have the same meanings as in the CCPA/CPRA, and
    iv. **Sub-Processor** means another processor engaged by the Processor to carry out specific processing activities with Personal Data.

CONTROLLER-PROCESSOR AND PROCESSOR-SUB-PROCESSOR RELATIONSHIPS

What are each party's obligations?

1. **Controller obligations.** Controller instructs Processor to process Personal Data in accordance with this DPA, and is responsible for providing all notices and obtaining all consents, licences and legal bases required to allow Processor to

process Personal Data. **Processor obligations.** Processor instructs Sub-Processor to process Personal Data in accordance with this DPA, and is responsible for sharing Controller's instructions with Sub-Processor prior to the processing of Personal Data.

2. **Processor obligations.** Processor will:

    a. only process Personal Data in accordance with this DPA and Controller instructions (unless legally required to do otherwise),

    b. not sell, retain or use any Personal Data for any purpose other than as permitted by this DPA and the Main Agreement,

    c. inform Controller immediately if (in its opinion) any instructions infringe Data Protection Laws,

    d. use the technical and organisational measures described in Annex 1 when processing Personal Data to ensure a level of security appropriate to the risk involved,

    e. notify Controller of a personal data breach within the Breach Notification Period and provide assistance to Controller as required under Data Protection Laws in responding to it,

    f. ensure that anyone authorised to process Personal Data is committed to confidentiality obligations,

    g. without undue delay, provide Controller with reasonable assistance with:

        i. data protection impact assessments,

        ii. responses to data subjects' requests to exercise their rights under Data Protection Laws, and

        iii. engagement with supervisory authorities,

    h. if requested, provide Controller with information necessary to demonstrate its compliance with obligations under Data Protection Laws and this DPA,

    i. allow for audits at Controller's reasonable request, provided that audits are limited to once a year and during business hours except in the event of a personal data breach, and

    j. return Personal Data upon Controller's written request or delete Personal Data by the end of the Term, unless retention is legally required.

3. **Warranties**. The parties warrant that they and any staff and/or subcontractors will comply with their respective obligations under Data Protection Laws for the Term.

4. **Sub-processing**

    a. **Use of sub-processors.** Controller authorises Processor engage other processors (referred to in this section as **sub-processors**) when processing Personal Data. Processor's existing sub-processors are listed in Annex 2.

    b. **Sub-processor requirements. Processor** will:

        i. require its sub-processors to comply with equivalent terms as Processor's obligations in this DPA,

        ii. ensure appropriate safeguards are in place before internationally transferring Personal Data to its sub-processor, and

        iii. be liable for any acts, errors or omissions of its sub-processors as if they were a party to this DPA.

c. **Approvals.** Processor may appoint new sub-processors provided that they notify Controller in writing in accordance with the Sub-processor Notification Period.

d. **Objections.** Controller may reasonably object in writing to any future sub-processor. If the parties cannot agree on a solution within a reasonable time, either party may terminate this DPA.

5. **International personal data transfers**

a. **Instructions.** Processor will transfer Personal Data outside the UK, the EEA or an adequate country only on documented instructions from Controller unless otherwise required by law.

b. **Transfer mechanism.** Where a party is located outside the UK, the EEA or an adequate country and receives Personal Data:

i. that party will act as the **data importer**,

ii. the other party is the **data exporter**, and

iii. the relevant Transfer Mechanism will apply.

c. **Additional measures.** If the Transfer Mechanism is insufficient to safeguard the transferred Personal Data, the data importer will promptly implement supplementary measures to ensure Personal Data is protected to the same standard as required under Data Protection Laws.

d. **Disclosures.** Subject to terms of the relevant Transfer Mechanism, if the data importer receives a request from a public authority to access Personal Data, it will (if legally allowed):

i. challenge the request and promptly notify the data exporter about it, and

ii. only disclose to the public authority the minimum amount of Personal Data required and keep a record of the disclosure.

6. **Other important information**

a. **Survival.** Any provision of this DPA which is intended to survive the Term will remain in full force.

b. **Order of precedence.** In case of a conflict between this DPA and other relevant agreements, they will take priority in this order:

i. Transfer Mechanism,

ii. DPA,

iii. Main Agreement.

c. **Notices.** Formal notices under this DPA must be in writing and sent to the Contact on the DPA's front page as may be updated by a party to the other in writing.

d. **Third parties.** Except for affiliates, no one other than a party to this DPA has the right to enforce any of its terms.

e. **Entire agreement.** This DPA supersedes all prior discussions and agreements and constitutes the entire agreement between the parties with respect to its subject matter and neither party has relied on any statement or representation of any person in entering into this DPA.

f. **Amendments.** Any amendments to this DPA must be agreed in writing.

g. **Assignment.** Neither party can assign this DPA to anyone else without the other party's consent.

h. **Waiver.** If a party fails to enforce a right under this DPA, that is not a waiver of that right at any time.

i. **Governing law and jurisdiction.** The Governing Law applies to this DPA and all disputes will only be litigated in the courts of the Jurisdiction.

MODULE 4 SCHEDULE TO THE DATA PROCESSING AGREEMENT

(Applicable for Controller Outside of the EEA)

VARIABLES	
Docking	Clause 7 of the Clauses apply
Redress	No changes are made to Clause 11 of the Clauses

APPENDIX TO THE CLAUSES

ANNEX I

A. LIST OF PARTIES	
Data exporter	
Name	As described in the Parties and Execution table at the beginning of this Schedule
Address	As described in the Parties and Execution table at the beginning of this Schedule
Contact person's name, position and contact details	As described in the Parties and Execution table at the beginning of this Schedule
Activities relevant to the data transferred under these Clauses	As described in the Variables table at the beginning of the DPA
Role	Controller
Data importer	
Name	As described in the Parties and Execution table at the beginning of this Schedule
Address	As described in the Parties and Execution table at the beginning of this Schedule

Contact person's name, position and contact details	As described in the Parties and Execution table at the beginning of this Schedule
Activities relevant to the data transferred under these Clauses	As described in the Variables table at the beginning of the DPA
Role	Controller

B. DESCRIPTION OF TRANSFER	
Term	***Description***
Data subjects. Categories of data subjects whose personal data is transferred	As described in the Variables table in the DPA
Personal data. Categories of personal data transferred	As described in the Variables table in the DPA
Sensitive data. 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	As described in the Variables table in the DPA
Transfer frequency. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	As described in the Variables table in the DPA
Nature of the processing	As described in the Variables table in the DPA
Purpose of the data transfer and further processing	As described in the Variables table in the DPA
Retention period. The period for which the personal data will be retained, or, if	As per the Main Agreement

that is not possible, the criteria used to determine that period	
Sub-processor transfers. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As described in Annex 2 of the DPA

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

On standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

STANDARD CONTRACTUAL CLAUSES

Controller to Controller

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) 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”).

3. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

4. 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.

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 8.1(b) and 8.3(b);

    iii. Clause 13;

    iv. Clause 15.1(c), (d) and (e);

    v. Clause 16(e);

    vi. 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

Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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, 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

Not applicable.

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 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

Not applicable.

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;

    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.

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 the Governing Law described in the Variables table of the DPA.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of the Jurisdiction described in the Variables table of the DPA.