Data Processing Addendum

Last Updated – 6 March 2026

Preamble

This Data Processing Addendum (hereinafter referred to as the "**Agreement**") supplements and is based on the contract (hereinafter referred to as the "**Main Contract**") concluded between the Client ("*Client Name* ", hereinafter is referred to as the "**Data Controller**", "Client") and the applicable BIPO entity (hereinafter is referred to as the "**Data Processor**", "BIPO") for the processing of Personal Data when providing Products and/or Services under the Main Contract.

Based on the Main Contract, the Data Processor provides one or more of the following services and/or software-as-a-service platforms to the Data Controller: Global Payroll Outsourcing (GPO) services, Employer of Record (EoR) services, Global Visa services, Contractor services, BIPO HRMS platform, Butter platform and other relevant BIPO platforms.

A Data Subject refers to any individual person who can be identified, directly or indirectly, via information related to the person (hereinafter referred to as "**Personal Data**" or "**Data**"), such as a name or an identity number. In this Agreement, Data Subjects may include prospective, current, and former employees of BIPO customers, as well as related persons like family members of the employees.

This Agreement will be effective on the effective signing date of the Data Processing Addendum ("**Effective Date**"). All capitalized terms not defined in this Agreement have the meanings set forth in the Main Contract. Both the Data Controller and the Data Processor are jointly referred to as the "**Parties**".

The Parties agree as follows:

§ 1 Scope of Application and Effectiveness

1.1 The Data Processor shall process Personal Data in accordance with the provisions of the Main Contract, this Agreement, and on behalf of and at the instruction of the Data Controller, for the purpose of fulfilling the performance obligations incumbent upon it under the Main Contract. Personal Data is as described in **Annex 1**.

1.2 The nature, scope, and purpose of the Data processing, the Personal Data itself and the group of Data Subjects are shown in **Annex 1**.

1.3 If the Data Processor is of the opinion that an instruction of the Data Controller violates Data Protection Laws, it shall notify the Data Controller thereof. In such cases, the Data

Processor shall be entitled to suspend the implementation of the instruction and shall not be liable to the Data Controller for failure to perform applicable services under the Main Contract until the Data Controller issues new and lawful instructions with regard to the processing of Personal Data.

§ 2 Obligations of the Data Controller

2.1 The Data Controller shall be responsible for compliance with all Data protection laws applicable to its use of the Platform and Services (as defined in the Main Contract), its Processing of Personal Data, and its Instruction to the Data Processor, its transfer of Personal Data to the Data Processor, the protection of the rights of the Data Subjects, including providing any necessary Notices and obtaining any necessary Consents and Authorizations. Should Data Subjects assert claims against the Data Processor based on the processing of their Data, the Data Controller shall indemnify the Data Processor against all such claims upon first request.

2.2 The Data Controller shall be solely responsible for: (i) the accuracy, quality, and legality of Personal Data and the means by which Data Controller acquired Personal Data that is disclosed or otherwise made available to Data Processor; (ii) ensuring Data Controller has the right to disclose or otherwise make available Personal Data to Data Processor for Processing

2.3 The Data Controller shall inform the Data Processor immediately and fully if it discovers any errors or irregularities in connection with the processing of the Data by the Data Processor under this Agreement or it's instructions.

§ 3 Obligations of the Data Processor

3.1 The Data Processor shall process the Data in accordance with the provisions of the Main Contract, this Agreement, and on the documented instructions of the Data Controller. It is not entitled to disclose the Data to third parties without authorization. This shall not apply if this (i) is done in accordance with the Agreement and the Main Agreement, (ii) is requested in writing by the Data Controller or (iii) is required by statutory or legal requirements. Data Processor shall, in cases under (iii), to the extent permitted by applicable law, inform Data Controller in advance of the intended disclosure and coordinate with Data Controller.

3.2 The Data Processor shall support the Data Controller in the event of inspections by the supervisory authorities within the scope of what is reasonable and necessary, insofar as these inspections concern Data processing by the Data Processor. It shall provide

the Data Controller with the information that the latter requires to prove that it has complied with the requirements of the applicable Data protection law with regard to this processing.

3.3 The Data Processor shall also support the Data Controller, taking into account the nature of the Data processing and the information available to it, upon request, in complying with the following Data Controller's obligations:

3.3.1 ensuring the security of Personal Data processing,
3.3.2 notification of Personal Data breaches to supervisory authorities and Data Subjects,
3.3.3 if necessary, carrying out a Data protection impact assessment, insofar as the Data processing by the Data Processor is affected by this,
3.3.4 if necessary, carrying out a required prior consultation with the Data protection authority, insofar as the Data processing by the Data Processor is affected by this.

3.4 The Data Processor shall inform the Data Controller without undue delay when it becomes aware of a Personal Data breach within the scope of its processing for the Data Controller.

3.5 The Data Processor shall require all personnel involved in data processing to maintain strict confidentiality, subject to disciplinary measures in case of non-compliance. Additionally, the Data Processor shall implement security safeguards comparable to those applied to its own personal information, in order to prevent unauthorized access by third parties.

3.6 The Data Processor may demand reasonable remuneration according to the Data Processor’s usual rates at the time for the cooperation services pursuant to Sections 3.2 and 3.3. However, this shall not apply to the cooperation pursuant to Section 3.3.2 if the violation is due to the Data Processor's fault.

§ 4 International Data Transfer

4.1 Where the Personal Data is transferred across borders, the Data Controller & Data Processor shall take necessary technical & organizational measures in order to ensure that such transfers are carried out with appropriate safeguards and according to the applicable data protection regulations.

4.2 Where the Personal Data is subject to the GDPR and Data is transferred outside EEA to a non-adequate country, according to chapter V of the GDPR and in order to ensure

an appropriate level of protection for the Data Subjects, EU Standard Contractual Clauses will be used. They are incorporated as **Annex 4.A** into this Agreement as follows:

4.2.1 If the Data Controller is the exporter and the Data Processor is the importer, the parties agree to use Module Two.

4.2.2 If the Data Processor is the exporter and the Data Controller is the importer, the parties agree to use Module Four.

4.3 Where the Personal Data is subject to the UK GDPR, the parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this Addendum (Annex 4) and completed as follows: References to the GDPR will be deemed to be references to the UK GDPR and the UK Data Protection Act 2018, references to "supervisory authorities" will be deemed to be references to the UK Information Commissioner, and references to "Member State(s)" or the EU will be deemed to be references to the UK. Annex 1 of this Addendum serves as Appendix I of the UK SCCs. Annex 2 of this Addendum serves as Appendix II of the UK SCCs.

§ 5 Technical and Organizational Measures

5.1 The Data Processor shall take the technical and organizational measures defined in **Annex 2** before the start of Data processing.

5.2 The technical and organizational measures are subject to technical progress and further development. In this respect, the Data Processor may implement alternative, adequate measures. Changes shall be documented, and the documentation shall be made available to the Data Controller upon request. The Data Controller shall be notified in writing of any significant changes. In the event of a material change, **Annex 2** shall be updated accordingly.

§ 6 Controls

6.1 The Data Controller shall review, at its own expense, prior to the commencement of Data processing by the Data Processor and thereafter on a regular basis, the implemented technical and organizational measures pursuant to **Annex 2** and shall document the respective result. The Data Controller shall also be entitled to carry out the audit in consultation with the Data Processor to the extent required. Notice of the inspection shall be communicated in advance and the inspection shall take place during the Data Processor's business hours. The Data Controller shall take the Data Processor's operational processes into account.

6.2 The Data Processor undertakes to provide the Data Controller, upon request, with the information required to perform a comprehensive review and to make the relevant evidence available. Evidence of the implementation of suitable measures can also be provided by submitting current test certificates as well as reports from independent auditors (auditor, audit, Data protection officer, IT security department, etc.). In this case, an on-site inspection by the Data Controller is excluded.

6.3 The Data Processor shall support the Data Controller as necessary for the purposes of the audit. The Data Processor may demand reasonable remuneration for its efforts in carrying out the audit.

§ 7 Subcontracting relationships

7.1 The Data Processor may establish subcontracting relationships with regard to the processing of the Data. The contractors and their respective areas of activity shall be listed in the **Main Contract**. The Data Controller shall be deemed to have consented to such relationships upon signing the Main Contract.

7.2 The Data Processor shall inform the Data Controller of any intended change of a subcontractor or addition of a new subcontractor.

7.3 The Data Processor shall pass on the obligations set out in this Agreement, including the guarantee of the technical and organizational measures, to its subcontractor. The technical and organizational measures shall comply with the requirements of the applicable Data protection law.

7.4 The Data Processor shall enter into a confidentiality or non-disclosure agreement with the subcontractors if they are not subject to a statutory confidentiality or non-disclosure obligation.

§ 8 Rights of Data Subjects

8.1 The rights of Data Subjects shall be asserted against the Data Controller.

8.2 Insofar as a Data Subject asserts their rights against the Data Processor, the Data Processor shall promptly forward the request to the Data Controller.

8.3 Insofar as a Data Subject asserts their rights against the Data Controller, the Data Processor shall support the Data Controller with suitable technical and organizational measures in the fulfillment of these claims appropriately and to the necessary extent if the Data Controller cannot fulfill the claim without the Data Processor's support.

8.4 The Data Processor may demand reasonable remuneration for the support activities pursuant to Section 8.3 of this Agreement.

8.5 Where Personal Data is disclosed by one party to a third party, the party shall ensure that it binds the third party to a comparable standard in handling, processing, and protecting the Personal Data, as required by applicable Data protection laws.

§ 9 Data protection officer (DPO)

If either parties have any queries/clarifications with regards to data protection or need to communicate on a data breach, the following DPO contact details are provided:
For the Data Processor: dpo@biposervice.com
For the Data Controller: *(Customer to fill)*

§ 10 Liability

10.1 The Data Processor shall be liable to the Data Controller for the violation of Data protection regulations and the provisions of this agreement in accordance with the relevant clauses in the Main Contract.

10.2 If claims are asserted against the Data Processor by third parties due to a violation of Data protection laws by the Data Controller, the Data Controller shall indemnify the Data Processor against liability upon first request. In addition, the Data Controller shall assist the Data Processor in its legal defense to the extent necessary and shall reimburse the Data Processor for all damages arising from the incident, including the reasonable costs of a legal defense.

§ 11 Contract Term and Return or Deletion of Data

11.1 The Agreement shall enter into force upon signature by both parties and shall run for an indefinite period. The Agreement shall end upon termination of the Main Contract, without the need for a separate termination of the Agreement.

11.2 If necessary, the parties shall agree on appropriate transitional arrangements in order to ensure the continuity of the processing operations beyond the end of the Main Contract.

11.3 Upon Data Controller's request, or upon termination or expiration of this Agreement, the Data Processor shall, upon Client's confirmation, destroy, and certify such deletion, or return to Client all Personal Data in its possession or control. This requirement shall not apply to the extent that the Data Processor is required by any applicable law to retain some or all of the Personal Data, in which event the Data Processor shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

11.4 Documentation which serves as evidence of the proper Data processing in accordance with the order shall be retained by the Data Processor in accordance with the relevant retention periods beyond the term of the Agreement. The same shall apply to other documents that are subject to legal retention obligations (e.g., under tax law).

§ 12 Miscellaneous

12.1 If the Data Controller's Data at the Data Processor is endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Data Processor shall inform the Data Controller thereof without undue delay. The Data Processor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the Data lie exclusively with the Data Controller as the responsible party.

12.2 In the event of changes to the actual form of the service relationships between the Parties, the Parties shall amend the Annexes accordingly and exchange them by mutual agreement. Upon signature of the amended Annex by the Parties, it shall become effective and replace the previously applicable Annex.

12.3 The Main Contract's provisions under the Service Agreement between Data Controller and Data Processor on governing law, arbitration and/or the legal venue apply.

12.4 Amendments or supplements to the agreement must be made in writing. This shall apply mutatis mutandis to any amendment or cancellation of the above written form requirement.

12.5 If individual provisions of this agreement are or become invalid, the validity of the remainder of the agreement shall not be affected. The invalid provision shall be replaced by a valid provision that comes as close as possible to the economic content of the invalid provision. The same shall apply in the event of loopholes.

§ 13 Joint Controllership (Below terms is only applied for Client with EOR services in EU or UK & where BIPO is the Employer of Record)

13.1 BIPO is a global payroll and people solutions provider and offers a total workforce solution that includes Employer of Record (EOR) services. Based on the Main Contract, the parties agree that for providing the EOR services, regarding the processing of the EOR employees' personal data, BIPO is also Data Controller because it is the Employer of Record. In this respect, if service delivery country is in EEA and/or UK, BIPO and the Client are **Joint Controllers** because they jointly determine the purposes and means of processing. The parties are aware that BIPO also acts as a Data Processor for the Client, as BIPO provides and maintains Butter and/or HRMS SaaS platform used by Client in providing the EOR services. If the EOR service delivery country is in any other country, BIPO is Data Processor and Client is Data Controller.

13.2 Joint Controllers for EOR Processing

13.2.1 BIPO and the Client are Joint Controllers and have jointly determined the means and purposes of processing Personal Data ("Joint Processing").

13.2.2 The Joint Processing shall solely be subject to the provisions of this Agreement. This Agreement determines the rights and obligations of both Parties.

13.2.3 This Agreement shall apply to all employees of the Parties as well as processors appointed by the Parties who perform processing of the Personal Data.

13.3 Means and Purposes of Joint Processing

The Parties agree that the means and purposes of the Joint Processing are as set out in **Annex 1.B** ("**Description of Data Processing**").

13.4 Rights and Responsibilities

13.4.1 Data Processing performed by the Parties shall be done according to purposes set out in Annex 1.B ("Description of Data Processing").

13.4.2 The Parties agree on the following responsibilities for compliance with data protection obligations towards Data Subjects with regard to the Joint Processing:

(a) The Parties shall provide the Data Subjects, upon request, with the essence of this Agreement. The essence of the Agreement may include only information that is necessary for the assertion of the Data Subjects' rights, but it should at least include: the name and address of the Joint Controllers (Parties), the purposes of the Joint Processing, the categories of the Data processed and, if applicable, the location of storage, the obligations of each Party, and the regulations for the Agreement termination.

(b) The Parties agree that they both shall be responsible for the fulfilment of the Data Subject's rights, depending on whether the Data Subjects assert their rights (with regard to the Joint Processing) against the Client or BIPO.

(c) The Parties agree that each shall maintain documentation of the Processing activities, throughout the Agreement period and beyond, in accordance with the legal obligations.

(d) Each Party, upon receiving a request for compensation for damage suffered by a Data Subject or a Third Party as a result of an infringement of applicable data protection law by the Joint Processing, shall notify the other Party about such a request, its intended response to such a request, and subsequently about the effected response and any further communication related to such a request to the extent permitted by law, without undue delay. Where the request for compensation requires information or an action by one of the Parties, such Party shall, upon the Data Subject's request and/or upon the other Party's request, provide such information or take such action without undue delay and to the extent necessary and reasonable.

13.5 When any of the Parties obtains Personal Data, such Party is responsible for ensuring that there is a valid legal basis for the Processing and for documenting this to both supervisory authorities and the data subject.

13.6 Each Party shall support the other Party in fulfilling its obligation to handle requests from Data Subjects regarding the exercise of their rights under applicable personal data protection laws and regulations.

13.7 Both Parties shall ensure that their employees involved in the processing maintain the confidentiality of the Personal Data for the duration of their employment or to the maximum term which is allowed under the applicable laws.

13.8 Each Party shall inform the other Party immediately and completely in case it detects failures or irregularities in connection with the Joint Processing within the framework of this Agreement.

13.9 Taking into account the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, each Party must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the relevant data protection laws.

13.10 Before transferring Personal Data of Data Subject to the other Party, or to Processors appointed by the Party in connection of the Joint Processing, each Party shall ensure the Data Subject has been informed about the transfer.

13.11 Data Breach Reporting Obligations as Joint Controllers

14. Each Party shall without undue delay notify the other Party of any personal data breach related to the processing that is the subject of this Agreement. The Parties shall provide each other with all information which is necessary for the assessment of the breach and its impact, as well as for the fulfilment of the applicable reporting and notification obligations to the relevant Supervisory Authority if required. The Parties shall support each other to a reasonable extent with the investigation and the remedial actions.

15. Should there be a duty to notify the Supervisory Authorities, the Parties shall coordinate to a reasonable extent and support each other in fulfilling the duty to notify.

16. In the event that a breach is likely to result in a high risk to the rights and freedoms of the Data Subjects concerned, the Party (concerned) shall communicate about the Data Breach to the Data Subjects without undue delay.

17. Neither Party shall make any Personal Data Breach public without the other Party's prior consent.

18. The Parties shall document any Personal Data Breaches, comprising the facts relating to the breach, its effects and the remedial action taken.

18.1 Responding to Inspections by Supervisory Authorities as Joint Controllers

19. The Parties agree that the Supervisory Authorities may, to the extent permitted by law, carry out inspections and, where appropriate, request the provision of information relating to this Agreement.

20. Each Party shall immediately inform the other Party if a Supervisory Authority contacts it and the request or the inspection concerns the Joint Processing under this Agreement.

21. The Parties shall coordinate the procedure and the response to the request and/or the performance of the inspection, to the extent that this is reasonable and legally permissible.

22. The Client shall pay BIPO's expenses with regard to the inspection or audit, unless the inspection or audit was caused by negligence or fraud by BIPO.

22.1 Data Subject Rights

23. If one of the Data Controllers receives a request from the Data Subject, the Parties will coordinate a response without undue delay, especially taking into account any relevant deadlines.

24. The parties are responsible for assisting each other to the extent this is relevant and necessary in order for both parties to comply with their obligations to the data subjects.

25. Each Party establishes and maintains a contact point for Data Subjects and for the other Party related to the Joint Processing.

25.1 International Data Transfer

26. BIPO operates as a global business and may transfer, store, or process personal data in a country outside of Data Subject's location/country .The Parties hereby agree that they are both authorized in their capacity as Joint Controllers of Personal Data to transfer the Personal Data internationally with suitable and appropriate safeguards and in accordance with applicable data protection law.

26.1 If Personal Data processed under this Agreement is transferred from a country within the European Economic Area (EEA) or UK to a country outside of the EEA or UK that does not have the European Commission's adequacy decision, the Parties have concluded the EU Standard Contractual Clauses as Annex 4.B to this agreement.

26.2 Liability as Joint Controllers

26.3 Regardless of the provisions of this Agreement, the Parties shall be jointly liable to the Data Subjects for damage caused by the processing of their Data in the framework of the Joint Processing under this Agreement that does not comply with applicable data protection law.

26.4 The Parties shall indemnify each other internally against any liability if the cause giving rise to liability is the sole responsibility of one Party in accordance with this Agreement. Where one or both Parties becomes liable to pay a fine and/or damages in respect of the Joint Processing, and notwithstanding anything to the contrary set forth in the MSA, each Party's contribution to the amount payable shall be determined in due proportion to their respective share of responsibility. To do so, the Parties shall discuss at the earliest convenience and agree on their respective contribution.

26.5 In the event any action by the Client leads to a claim against BIPO, the Client will immediately indemnify BIPO and hold BIPO harmless from any such claims so that BIPO will not have to settle such claims upfront.

26.6 For the sake of clarity, BIPO is jointly and severally liable only to the extent mandated by applicable laws and regulations. In other scenarios, BIPO is only liable for the actual liability arising from BIPO's own fault.

Annex 1: Data, Data Subjects, Data processing and purpose of Data processing
Annex 2: Technical and organizational measures
Annex 3: Approved subcontractors and areas of activity of the subcontractor
Annex 4.A: Standard Contractual Clauses
Annex 4.B: Standard Contractual Clause (Only applicable for Client with EOR services in EU or UK & where BIPO is the Employer of Record)

Insert Signature Place Holder
(similar to MSA signed with same signing entities & signatories)

Annex 1.A: List of Parties

1. For transfer from Controller to Processor:

Data Exporter	**Data Importer**
Name: Client	Name: BIPO
Address/Email: As provided for in the Main Contract	Address/Email: As provided for in the Main Contract
Contact Person's name, position, and contact details: As provided for in the Main Contract	Contact Person's name, position, and contact details: As provided for in the Main Contract
Activities relevant to transfer: see Annex 1.B	Activities relevant to transfer: see Annex 1.B
Role: Controller	Role: Processor

Annex 1.B: Description of Processing

Data Subjects may include	*(To be edited by the Client)* ✓ Prospective, current, and former employees, as well as related persons like family members of the employees. ✓ Employer of Record employees ✓ Contractors, the independent freelancer who sign the service agreement with BIPO to perform the services assigned by BIPO's clients
Categories of Personal Data	Prospective, current, and former employee Data *(The list is not exhaustive - to be edited by the Client as required. Sensitive data (like Ethnicity, Citizenship, Religion, Nationality, Visa details, Medical certificates – if not stored/processed – kindly remove from list)* Employee Data that is necessary for human resources and benefits processing, including name, contact information (including home and work address, home and work telephone numbers, mobile telephone numbers, home and work email address), marital status, birth date, gender, Ethnicity, Citizenship, Religion, Nationality, Visa details, Medical certificates, employee position title, business title, resume, job grade or code, business site, company, supervisor, cost center, work schedule, employment status (full-time or part-time, regular or temporary), compensation and related information, payroll information, bank account information , allowance, bonus, attendance records, performance reviews and appraisals, leave applications , claims and disbursements, emergency contact information ,work experience information, training and development information. Related Person/Dependent's Information Related person's Data, such as name and contact information of dependents or beneficiaries (including home address, home and work telephone numbers, mobile telephone numbers, date of birth, gender, emergency contacts, beneficiary information, dependent information)
Frequency of Processing	Continuous
BIPO Systems locations	*(BIPO to update* *example: HRMS – Singapore, Butter – Frankfurt)*

Integration	*(Client to update)* *(Purpose,* *Inbound & Outbound transfer details* *& Client system location)*
Countries in scope for processing	As mentioned in the Service Agreement
Services Accepted	As mentioned in the Service Agreement
Purpose of Processing	Provisioning of services (as mentioned in SOW of Main Services Agreement
Duration of Processing	Length of the Service Agreement
Retention	Personal data will be retained as needed to fulfill the purposes for which it was collected, such as delivery of the Services and Products, and as necessary for BIPO to comply with its business requirements, legal obligations, resolve disputes, protect its assets, and enforce its rights and agreements.

Annex 1.C: Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with Clause 12: The competent supervisory authority is the (*name of data protection supervisory authority*) of (*Country/Region name*) or any successor authority responsible for overseeing the implementation and enforcement of data protection laws in (*Country/Region name*).

It is the competent supervisory authority/ies in accordance with Clause 12 who has the responsibility for ensuring compliance by the data exporter.

Annex 2: Technical and Organizational Measures

The Data Processor has adopted technical and organizational measures to ensure that processing activities under this Agreement are carried out in compliance with applicable Data protection provisions.

The Data Processor has adopted security measures to guarantee protection standards adequate to the risks to confidentiality, integrity, availability, and resilience of the systems, taking into account the likelihood of data breaches and the severity of risk to the rights and freedoms of natural persons possibly resulting thereof.

Technical and organizational measures shall always be monitored and updated according to the technical progress and development in order to maintain or increase the Data protection standards.

Following are the security measures for BIPO SaaS Applications:

1. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:
- Non-disclosure agreements;
- Information security policies and procedures;
- Input validation and database integrity constraints
- Backup and restore testing procedures;
- Highly available and fault-tolerant backup storage;
- Anti-virus/firewall protection, security patch management;
- System availability and exceptions monitoring and detection;
- Periodic user access reviews;

2. Measures of encryption and protection of Personal Data:
- Encryption at rest and encryption in transit.
- Use of data masking to mask personal information for troubleshooting purposes.

3. Measures for user identification and authorization:
- Internal policies and procedures on user accounts and user access requests.
- User access control, user authentication.
- Access granted based on a need-to-know.
- Logging of user activity and data change.

4. Measures for the protection of data during storage:
- Encryption at rest;
- Access controls;
- Physical and logical segmentation of data from different customers.
- Separation of environments (production/testing/development);

5. Measures for ensuring the ability to recover the service in a timely manner in the event of disaster:
- Business continuity plan;

- Disaster recovery procedure;
- Incident response plan;

6. Measures for ensuring events logging
- System audit logs enablement
- Secure log storage and retention
- Access control to restrict log access to authorized personnel only

7. Measures for ensuring system configuration, including default configuration
- Secure default configurations
- Enable encryption by default

8. Measures for certification/assurance of processes and products
- ISO27001 certification SOC1 and SOC2 Type II audit reports
- Third party vendor assurance
- Annual penetration testing

9. Measures for ensuring limited data retention
- Contractual clause and policies outlining retention timelines
- Secure deletion method

10. Measures for ensuring accountability
- Regular reviews of data protection policies and procedures,
- Adopting legal requirements into policies and practices,
- Privacy by design implementation
- Regular audits

11. Measures for allowing data portability and ensuring erasure
- System features to facilitate data export
- Data purge feature

12. Measures for ensuring the effectiveness of technical and organizational measures:
- Physical environment security policy;
- Door access control system;
- Surveillance facilities (CCTV, alarm system);
- Locked cabinets, secure location of critical equipment;

Annex 3: List of Sub-processors

BIPO may use Sub-processors when it acts as Processor. The list of sub processors for a particular client will be mentioned in the Appendix section of the Main Service Agreement signed with the client.

Services which the parties use with third parties as an ancillary service to support the execution of the Project, e.g. telecommunications services, cloud hosting services, ticketing platform etc are not regarded as services of subcontractors within the meaning of this provision.

Annex 4.A: Standard Contractual Clauses

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)[1] for the transfer of Personal Data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the Personal Data, as listed in Annex I.A. (hereinafter each "Data exporter"), and

(ii) the entity/ies in a third country receiving the Personal Data from the Data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "Data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of Personal Data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and Invariability of the Clauses

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

---

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

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

Clause 3

Third-Party Beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the Data exporter and/or Data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module Two: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Module Two: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of Data Subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the Transfer(s)

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

Clause 7 - Optional

Docking Clause

(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.

MODULE TWO: Transfer from Controller to Processor

8.1 Instructions

(a) The Data importer shall process the Personal Data only on documented instructions from the Data exporter. The Data exporter may give such instructions throughout the duration of the contract.

(b) The Data importer shall immediately inform the Data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of Processing and Erasure or Return of Data

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

8.6 Security of Processing

(a) The Data importer and, during transmission, also the Data exporter shall implement appropriate technical and organisational measures to ensure the security of the Data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that Data (hereinafter "Personal Data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the Data Subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the Personal Data to a specific Data Subject shall, where possible, remain under the exclusive control of the Data exporter. In complying with its obligations under this paragraph, the Data importer shall at least implement the technical and organisational measures specified in Annex II. The Data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The Data importer shall grant access to the Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a Personal Data breach concerning Personal Data processed by the Data importer under these Clauses, the Data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The Data importer shall also notify the Data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The Data importer shall cooperate with and assist the Data exporter to enable the Data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected Data

Subjects, taking into account the nature of processing and the information available to the Data importer.

8.7 Sensitive Data

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

8.8 Onward Transfers

The Data importer shall only disclose the Personal Data to a third party on documented instructions from the Data exporter. In addition, the Data may only be disclosed to a third party located outside the European Union[2] (in the same country as the Data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the Data Subject or of another natural person.

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

8.9 Documentation and Compliance

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

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the Data importer shall keep appropriate documentation on the processing activities carried out on behalf of the Data exporter.

(c) The Data importer shall make available to the Data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the Data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-

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

compliance. In deciding on a review or audit, the Data exporter may take into account relevant certifications held by the Data importer.

(d) The Data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the Data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer from Processor to Controller

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[3], 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.

---

[3] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

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

MODULE TWO: Transfer from Controller to Processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The Data importer shall not subcontract any of its processing activities performed on behalf of the Data exporter under these Clauses to a sub-processor without the Data exporter's prior specific written authorisation. The Data importer shall submit the request for specific authorisation at least thirty (30) days prior to the engagement of the sub-processor, together with the information necessary to enable the Data exporter to decide on the authorisation. The list of sub-processors already authorised by the Data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The Data importer has the Data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The Data importer shall specifically inform the Data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the Data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The Data importer shall provide the Data exporter with the information necessary to enable the Data exporter to exercise its right to object.

(b) Where the Data importer engages a sub-processor to carry out specific processing activities (on behalf of the Data exporter), it shall do so by way of a written contract that provides for, in substance, the same Data protection obligations as those binding the Data importer under these Clauses, including in terms of third-party beneficiary rights for Data Subjects.[4] The Parties agree that, by complying with this Clause, the Data importer fulfils its obligations under Clause 8.8. The Data importer shall ensure that the sub-processor complies with the obligations to which the Data importer is subject pursuant to these Clauses.

(c) The Data importer shall provide, at the Data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the Data exporter. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Data importer may redact the text of the agreement prior to sharing a copy.

(d) The Data importer shall remain fully responsible to the Data exporter for the performance of the sub-processor's obligations under its contract with the Data importer. The Data importer shall notify the Data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The Data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the Data importer has factually disappeared, ceased to exist in law or has become insolvent - the Data exporter shall have the right to terminate the

[4] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

sub-processor contract and to instruct the sub-processor to erase or return the Personal Data.

Clause 10

Data Subject Rights

MODULE TWO: Transfer from Controller to Processor

(a) The Data importer shall promptly notify the Data exporter of any request it has received from a Data Subject. It shall not respond to that request itself unless it has been authorised to do so by the Data exporter.

(b) The Data importer shall assist the Data exporter in fulfilling its obligations to respond to Data Subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the Data importer shall comply with the instructions from the Data exporter.

MODULE FOUR: Transfer from Processor to Controller

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.

[OPTION: The Data importer agrees that Data Subjects may also lodge a complaint with an independent dispute resolution body[5] at no cost to the Data Subject. It shall inform the Data Subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE TWO: Transfer from Controller to Processor

(b) In case of a dispute between a Data Subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

[5] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(c) Where the Data Subject invokes a third-party beneficiary right pursuant to Clause 3, the Data importer shall accept the decision of the Data Subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the Data Subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The Data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The Data importer agrees that the choice made by the Data Subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE FOUR: Transfer from Processor to Controller

(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.

MODULE TWO: Transfer from Controller to Processor

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

(b) The Data importer shall be liable to the Data Subject, and the Data Subject shall be entitled to receive compensation, for any material or non-material damages the Data importer or its sub-processor causes the Data Subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the Data exporter shall be liable to the Data Subject, and the Data Subject shall be entitled to receive compensation, for any material or non-material damages the Data exporter or the Data importer (or its sub-processor)

causes the Data Subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the Data exporter and, where the Data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the Data exporter is held liable under paragraph (c) for damages caused by the Data importer (or its sub-processor), it shall be entitled to claim back from the Data importer that part of the compensation corresponding to the Data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the Data Subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the Data Subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The Data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer from Controller to Processor

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

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

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

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

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

Clause 14

Local Laws and Practices Affecting Compliance with the Clauses

MODULE TWO: Transfer from Controller to Processor

MODULE FOUR: Transfer from Processor to Controller *(where the EU processor combines the Personal Data received from the third country-controller with Personal Data collected by the processor in the EU)*

(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[6];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied

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

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

MODULE TWO: Transfer from Controller to Processor

MODULE FOUR: Transfer from Processor to Controller *(where the EU processor combines the Personal Data received from the third country-controller with Personal Data collected by the processor in the EU)*

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) [For Module Four: 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

MODULE TWO: Transfer from Controller to Processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the country mentioned in the Main Contract if the conditions of the first sentence are met, otherwise Germany.

MODULE FOUR: Transfer from Processor to Controller

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 country mentioned in the Main Contract if the condition of the first sentence are met, otherwise Germany.

Clause 18

Choice of Forum and Jurisdiction

MODULE TWO: Transfer from Controller to Processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany .

(c) A Data Subject may also bring legal proceedings against the Data exporter and/or Data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer from Processor to Controller

Any dispute arising from these Clauses shall be resolved by the courts of the country mentioned in the Main Contract or, if not applicable by law, by German Courts

Annex 4.B: Standard Contractual Clauses

Controller-to-Controller Data Transfers

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) ([7]) for the transfer of personal data to a third country.

b) The Parties:

i) the natural or legal legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

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

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

[7] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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 8.5 (e) and Clause 8.9(b);

   iii) Clause 12(a) and (d);

   iv) Clause 13;

   v) Clause 15.1(c), (d) and (e);

   vi) Clause 16(e);

   vii) Clause 18(a) and (b);

b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Purpose limitation

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

i) where it has obtained the data subject's prior consent;

ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

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

i) of its identity and contact details;

ii) of the categories of personal data processed;

iii) of the right to obtain a copy of these Clauses;

iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

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

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

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

8.3 Accuracy and data minimization

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

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

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

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymization ([8]) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from

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

whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union ([9]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

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

ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

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

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

Clause 10

Data subject rights

a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these

Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([10]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

b) In particular, upon request by the data subject the data importer shall, free of charge:

   i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

   ii) rectify inaccurate or incomplete data concerning the data subject;

   iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

   i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

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

ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

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

Clause 11

Redress

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

b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

ii) refer the dispute to the competent courts within the meaning of Clause 18.

d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

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

b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([11]);

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

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.

g) 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 minimization

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

b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii) the data importer is in substantial or persistent breach of these Clauses; or

   iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the

data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the country mentioned in the Main Contract if the conditions of the first sentence are met, otherwise Germany.

Clause 18

Choice of forum and jurisdiction

a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b) The Parties agree that those shall be the courts of the country mentioned in the Main Contract if the conditions of the first sentence are met, otherwise Germany.

c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I – DESCRIPTION OF PROCESSING & DATA TRANSFERS

See **Annex 1** of the DPA

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

See **Annex 2** of the DPA

ANNEX III – LIST OF SUB-PROCESSORS

See **Annex 3** of the DPA