# General Binding Conditions for Personal Data Processing by the Processor and Other Parties

## CONTENTS

## I. Introductory provisions

In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to as the "***GDPR***"), the following General Binding Conditions for Personal Data Processing by the Processor and Other Parties (hereinafter also referred to as "***Processing Conditions***") come into effect on 25 May 2018.

These Processing Conditions have been adopted together with other documents regulating the rights and obligations in connection with the protection of personal data at **Smartwings, a.s., ID No.: 25663135, registered office in Prague 6, K Letišti 1068/30, 160 08** *(hereinafter referred to as "**SW CZ**")*. SW CZ is the parent company of the other joint Controllers, namely **Smartwings Slovakia, s.r.o.**, registered office at Ivanská cesta 30/B, Bratislava 821 04 (hereinafter referred to as "*SW SK*"), Smartwings Hungary Kft., registered office at Wesselényi u. 16/A, Budapest, 1077, Hungary (hereinafter referred to as "SW HU"), Smartwings Poland Sp. z o.o., registered office at ul. Gordona Bennetta 2B, Warszawa, 02-159, Poland (hereinafter referred to as "SW PL") and Smartwings Germany Gmbh, registered office at Germendorfer Allee 55, c/o ASE Office, 16515 Oranienburg, Germany (hereinafter referred to as "SW DE") (all hereinafter collectively referred to as "SW", or the "Controller"). These Conditions govern each Controller's relationship with the Processor individually, under the circumstances of the primary agreement, unless a written processing agreement has been concluded between the Parties that deviates from the provisions of these Terms.

The Controller shall conclude a written Personal Data Processing Agreement with each Processor (hereinafter also referred to as the "***Processing Agreement***"), which shall make binding reference to these Processing Conditions. Unless a written Processing Agreement is concluded with the Processor, the relationship established by the Primary Agreement shall always be governed by these Processing Conditions, and these Conditions shall become part of the Primary Agreement.

**These Processing Conditions bindingly regulate the rights and obligations of the Controller and the Processor in the processing of personal data of data subjects by the Processor for the Controller in connection with the Service performed by the Processor for the Controller or the Products provided by the Processor to the Controller.** Processors are

obliged to become familiar with these Processing Conditions and to process personal data in accordance herewith. In addition to the Processor's obligation to process personal data in accordance with these Processing Conditions, the Processing Agreement will specify in particular the personal data pursuant to the first sentence of Article 28(3) GDPR. In the event of a need arising from the provision of a particular Service or Product, the obligations and rights of the Parties in the Processing Agreement may be governed differently from these Processing Conditions, in which case the different provision in the Processing Agreement shall prevail.

A specimen of the Processing Agreement is included in these Processing Conditions as **Annex No. 1**.

Unless specified otherwise in the Processing Agreement, the contact person responsible for the personal data protection agenda for the purposes of personal data processing by the Processor, i.e. the person designated to communicate and provide assistance between the Controller and the Processor, is each of the joint Controllers separately, at the registered office of the specific Controller published in the public register. The joint Controllers have also designated the following as a common point of contact: **Smartwings, a.s., ID No.: 25663135, registered office at Prague 6, K Letišti 1068/30, 160 08, Czech Republic, e-mail address law@smartwings.com.**

The authorised representative of SW CZ is:

KUBEČKA & PROKOP, advokátní kancelář s.r.o., registered office at Kladská 1489/5, Vinohrady, 120 00 Prague 2, Czech Republic, e-mail: dpo@smartwings.com.

## II. Definitions

1. For the purposes of the Processing Conditions and other related personal data protection documents, the Controller uses the terms:
    - **"Controller"** means Smartwings, a.s., ID No.: 25663135, registered office at Prague 6, K Letišti 1068/30, Postal Code 16008, Czech Republic or Smartwings Slovakia, s.r.o., registered office at Ivanská cesta 30/B, Bratislava 821 04, Slovak

Republic, Smartwings Hungary Kft., registered office at Wesselényi ul. 16/A, Budapest, 1077, Hungary, Smartwings Poland Sp. z o.o., registered office at ul. Gordona Bennetta 2B, Warszawa, 02-159, Poland, or Smartwings Germany Gmbh, registered office at Germendorfer Allee 55, c/o ASE Office, 16515 Oranienburg, Germany, depending on the circumstances of the Primary Agreement;

- "**Personal data**" means any information about an identified or identifiable natural person (*hereinafter referred to as a* "***Data Subject***") provided by the Controller to the Processor or provably identifiable subject thereof, and processed by the Processor for the Controller pursuant to and/or in connection with the Primary Agreement;
- "**Processor**" means any entity processing personal data for and on behalf of the Controller;
- "**Sub-processor**" means any other processor of personal data (including any third party) engaged by the Processor to process personal data on behalf of the Controller. The Processor and the Sub-processor are entitled to engage another Sub-processor in the processing of personal data under the conditions set out in these Processing Conditions;
- "**Approved Sub-processor**" means (a) the Sub-processor listed in Annex No. 3 to the personal data Processing Agreement (transfer of personal data previously authorised by the Controller); and (b) other Sub-processors authorised in writing in advance by the Controller in accordance with Article IX of these Processing Conditions;
- "**Primary Agreement**" means a valid and effective legal transaction entered into between the Controller and the Processor under which the Processor performs a particular Service or provides certain Products (as specifically defined in the Processing Agreement) for the Controller;
- "**Instruction**" means any instruction from the Controller to the Processor regarding the processing of personal data. The Processor is obliged to prove the existence and content of the Instruction at any time during the processing of personal data;

- “**Personal data security breach**” - a personal data security breach which leads or may directly lead to the accidental, unauthorised or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.
- "**Data Protection Regulations**" means the GDPR and any legal regulations concerning personal data at national level and in the European Economic Area or the EU, which applies to the Controller or Processor;
- "**Standard contractual clauses**" means the standard contractual clauses for the transfer of personal data to processors domiciled in third countries, approved by European Commission Decision 2010/87/EU of 5 February 2010, or any set of provisions approved by the European Commission which amends, supplements or replaces them;
- "**Third country**" means any country outside the EU or the European Economic Area, except where that country is subject to a valid and effective European Commission decision on the adequate protection of personal data in third countries;
- "**Erasure**" means the irreversible removal or destruction of personal data so that they cannot be restored or reconstructed;
- "**Principles of personal data processing**" are the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality as defined in the GDPR.
- “**Significant supplier**” means the operator of an information or communication system and any party that enters into a legal relationship with the Controller that is significant in terms of the security of the information and communication system. A significant supplier shall be demonstrably informed in writing that it is registered as a significant supplier.

2. **Any other general terms not mentioned or defined in these Processing Conditions, the Processing Agreement, the Primary Agreement or other documents adopted by the Controller in connection with the protection of personal data shall be interpreted in accordance with the GDPR.**

## III. General Conditions of Personal Data Processing by the Processor

1. **The Processor is authorised to process personal data for the Controller on the latter's behalf during the performance of the Primary Agreement in accordance with and subject to the conditions stipulated in these Processing Conditions, unless otherwise stipulated in the Processing Agreement, the Controller's Instructions and Data Protection Regulations.**
2. **The Processor is authorised to process personal data only for the purpose of performing the Primary Agreement or for the performance provided under the Primary Agreement. The purpose of processing and other conditions of processing are determined by the Controller, and should the Processor violate this rule, it shall be deemed to be a controller in relation to such processing. The specific purpose of processing and other specifications of processing are regulated in the Processing Agreement.**
3. The Processor undertakes to comply with all technical and organisational measures to ensure compliance with the requirements set out in these Processing Conditions, the Data Protection Regulations and the Processing Agreement. The technical and organizational measures for the purposes of personal data processing are defined in Annex No. 2 to these Processing Conditions, with the option of further specification in the Processing Agreement.
4. The Processor is obliged to procure, renew and maintain all necessary licenses, authorizations and permissions needed to process personal data, as required by the applicable and effective Data Protection Regulations.
5. The Processor is obliged to inform the Controller immediately, but no later than within 3 days of delivery of the Instruction, that it believes the Instruction does not comply with the Data Protection Regulations, the Processing Agreement, these Processing Conditions or otherwise violates them.

## IV. Transfer of personal data and processing in a third country

1. The Processor is not authorised to process/enable processing, in particular to transfer, disseminate, modify, disclose, alter, publish or authorise the publication or

otherwise make personal data available to any third party other than in accordance with these Processing Conditions, the Processing Agreement or the Instructions, except for the transfer of personal data required by EU or Member State law (*hereinafter also referred to as a "**legal requirement to transfer**"*), to which the Processor is subject. The Processor is obliged to inform the Controller of the legal requirement to transfer personal data sufficiently in advance of the transfer, unless the applicable law prohibits notification of the transfer of personal data.

2. The Processor is obliged to minimise the scope of transferred personal data, unless the applicable legislation mandatorily regulates the scope of transferred personal data.

3. The Processor is not authorised to process personal data in a third country without prior written consent from the Controller, even through a Sub-processor, unless stipulated otherwise below or in the Processing Agreement.

4. Processors are automatically authorised to transfer personal data to the recipients in third countries and international organisations listed in Annex 3 of these Processing Conditions (*hereinafter also referred to as "**Controller-approved transfer of personal data**"*) for the purpose of their processing, provided that such parties comply with the requirements set out in Article IX of these Processing Conditions. The Processor is obliged to inform the Controller of the transfer of personal data to the Controller-approved parties listed in Annex No. 3 without delay, but no later than within 3 days.

5. The Processor is obliged, upon the request from the Controller, to promptly conclude an agreement with the Controller, including Standard Contractual Clauses or similar clauses as may be required by the Data Protection Regulations, in respect of any personal data processing in a third country. The Processor is obliged to ensure that any other Sub-processor also concludes the legal act according to the previous sentence with the Controller.

## V. Authorised persons processing personal data with the Processor

1. The Processor is obliged to take all necessary measures to screen its employees or other persons who process personal data with the Processor. The Processor is obliged to provide access to personal data only to screened and reliable employees

or other persons (*hereinafter also referred to as "**Authorised Persons**"*) and only to the extent necessary for the performance of the Primary Agreement. The Processor shall regularly screen Authorised Persons and review their reliability.

2. The Processor maintains a list of Authorised Persons with access to personal data and regularly updates it to reflect reality.
3. The Processor is obliged to inform the Authorised Persons that the personal data are data subject to protection under the Data Protection Regulations, the processing of which is governed by the Data Protection Regulations and the obligations set out in the Processing Conditions, the Processing Agreement and the Instructions. The Processor is obliged to explain the obligations under the preceding sentence to the Authorised Persons in a clear and unambiguous manner and to oblige them to comply therewith.
4. The Processor is obliged to maintain the confidentiality of personal data and their processing by the Controller and the Processor. The Processor is obliged to contractually bind the Authorised Persons to a nondisclosure obligation for the duration of employment or other legal relationship between the Processor and the Authorised Person, including for a reasonable period of time after the termination of such relationship, in the event that they are not subject to a legal or professional nondisclosure obligation, in which case the Processor is obliged to inform the Authorised Persons of their legal/professional nondisclosure obligation.
5. The Processor is obliged to provide regular and adequate training and certification for Authorised Persons in connection with the Data Protection Regulations and/or the Instructions.
6. The Processor is obliged to ensure that the Authorised Persons, when processing personal data, in particular:
    - use only secure hardware and software and observe the principles of safe use of computer equipment;
    - be subject to and adhere to user authentication and login processes when accessing personal data;

- prevent the unauthorised reading, destruction, deletion or other loss, alteration or disclosure of personal data, not make copies of personal data media for other than business use, and not allow such conduct by others, including other unauthorised disclosure or provision;
- immediately, but no later than 24 hours after the occurrence, report any reasonable suspicion of a threat to the security of personal data to the person referred to in Article 1 of these Processing Conditions.

## VI. Processor’s cooperation in fulfilling the Controller's obligations

1. The Processor is obliged to cooperate with the Controller in fulfilling the Controller's obligations to data subjects, including responding to requests to exercise the rights of data subjects under the Data Protection Regulations and through appropriate technical and organisational measures, and in fulfilling the Controller's other obligations under the Data Protection Regulations.
2. The Processor is obliged to cooperate within a reasonable period of time, unless a specific time limit is specified in these Processing Conditions, the Processing Agreement or the Controller's Instruction.
3. For the purposes of these Processing Conditions, cooperation means assistance in ensuring compliance with the obligations under Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to the Processor, and only in relation to personal data processing.
4. Cooperation includes in particular:
   - providing and disclosing all information, data and documents relating to personal data or necessary to demonstrate compliance with the applicable and effective Data Protection Regulations, these Processing Conditions, the Processing Agreement and the Instructions;
   - assistance and consultancy by the Processor that is reasonable and proportionate in relation to the specific obligation to which the Controller is subject;

- implementation of additional technical and organisational measures that the Controller may reasonably require beyond its legal and contractual obligations in order to respond effectively to complaints, communications or requests;
- assistance in all data protection impact assessments required under Article 35 GDPR and with any prior consultation with any supervisory authority of the Controller required under Article 36 GDPR.

5. The Processor is obliged without undue delay, but no later than 7 days after receipt of the request, to notify the data subject, supervisory authority or other entity that it has received a request under the Data Protection Regulations relating to personal data.
6. The Processor is obliged to allow audits and inspections by the Controller or another auditor authorised by the Controller (*hereinafter also referred to as the "**authorised auditor**"*) in all places where personal data are processed. The Processor shall cooperate and allow the Controller/authorised auditor to inspect, audit and copy all records, processes and systems so that the Controller can verify that personal data processing complies with the applicable and effective Data Protection Regulations, these Processing Conditions, the Processing Agreement and the Instructions.
7. The Processor is obliged to provide and hand over to the Controller documents relating to personal data processing and the fulfilment of the Processor's obligations.
8. The Processor shall notify the Controller immediately if, in its opinion, the right to audit under this article is in breach of the Data Protection Regulations.
9. The Processor is obliged to ensure the exercise of the Controller's rights under this article also for all its Sub-processors.

## VII. Securing of personal data

1. In accordance with Art. 32(1) GDPR, i.e. with regard to the condition of equipment, cost for performance, nature, scope, context and purpose of processing, as well as various probably and various serious risks for the rights and freedoms of natural persons, the Controller shall implement suitable technical and organisation measures in order to ensure a degree of security corresponding to the given risk.

2. During personal data processing, the Processor is obliged to a reasonable extent to ensure at the least:
    - the pseudonymisation and encryption of personal data
    - the ongoing confidentiality, integrity, availability and resilience of personal data processing systems and services;
    - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    - the regular testing, assessment and evaluation of the efficacy of technical and organisational measures for ensuring the secure processing of personal data;

    where the specific terms and conditions for the personal data security are contained in Annex No. 2 to these Processing Conditions and may be further specified in the Instruction or the Processing Agreement.
3. Unless there is a written Processing Agreement between the parties to the Primary Agreement, or an annex to the Primary Agreement or Processing Agreement which expands on these technical and organisational measures, Article 7 of these Conditions is the minimum level of measures that the Processor must take.
4. When assessing the suitable security level, the Controller will take particular account of the risks posed by personal data processing, in particular the random or unlawful destruction, loss, alteration, unauthorised disclosure of transferred, stored or otherwise processed personal data, or unauthorised access to them.
5. In the case of processing personal data for multiple controllers, the Processor is obliged to process the Controller's personal data separately so as to prevent their mixing and joint processing.

## VIII. Personal data security breach

1. In the event of a personal data security breach, the Processor is obliged to notify the Controller immediately, but no later than within 24 hours, that a personal data security breach has occurred or that there is a reasonable suspicion of a personal data security breach (hereinafter also referred to as "***security breach notification***").

2. The Processor is obliged to provide the Controller with sufficient information to enable the Controller to comply with any obligations relating to the reporting and notification of personal data security breaches under the Data Protection Regulations. At a minimum, the security breach notification must include:
    - a description of the nature of the specific personal data security breach and, where possible, the categories and number of data subjects affected and the number and specification of the personal data records affected;
    - the name and contact details of the Processor's Data Protection Officer or other entity from which more information can be obtained;
    - description of the probable consequences of the personal data security breach and resulting risk;
    - description of the measures taken or proposed to address the security breach;
    - description of the measures taken or proposed to mitigate the potential adverse effects of the security breach.
3. The Processor shall cooperate with the Controller, provide the Controller with all possible assistance to investigate, mitigate, eliminate and rectify the personal data security breach and implement the Controller's Instructions for this purpose.
4. The entity responsible for reporting a personal data security breach under the Data Protection Regulations is the Controller. The Processor is not authorised to notify any entity of a personal data security breach without prior demonstrable consent from the Controller, unless the Processor is obliged to do so under EU or Member State law to which the Processor is subject. The Processor shall promptly, and prior to providing notice, inform the Controller of the legal requirement to report the personal data security breach. The Processor shall provide the Controller with the text of the notice for the Controller's comments in advance and well before the expiry of any deadline applicable to the Processor for the purpose of reporting the security breach. The Processor is obliged to modify the notice in accordance with the Controller's Instructions, provided they comply with EU and Member State law applicable to the Processor and correspond to the security breach that has occurred.

The Processor is required to consider any further comments the Controller may have regarding the notice.

## IX. Sub-processors

1. Based on these Conditions, the Controller grants the Processor general authorisation to engage another processor for processing on the basis of the Primary Agreement, except where:

   a) there is no written Processing Agreement between the Controller and the Processor, which includes these Conditions;

   b) the written agreement between the Controller and the Processor excludes processing by another processor, or specifies otherwise;

   c) processing by the Sub-processor takes place in third countries and there is no Commission decision on an adequate level of personal data protection or other bilateral or multilateral international treaty guaranteeing this adequate level of protection of personal data.

   d) The Controller has withdrawn its consent, even after processing has begun, because it believes the engaged Sub-processor does not meet these Conditions.

2. The Processor may engage another Sub-processor in personal data processing even if it cannot engage them in the processing pursuant to the previous paragraph of this article, provided that such entities are listed in the document, a specimen of which is set out in Annex 3 to these Processing Conditions (Approved Sub-processor). The Processor is obliged to inform the Controller of the engagement of the Approved Sub-processor listed in Annex 3 promptly, but no later than 3 days prior to the intended engagement. The Controller is authorised to withdraw its consent to the engagement of a further processor at any time and may also unilaterally exclude the approved Sub-processor from further processing because it believes the involved Sub-processor does not comply with these Conditions.

3. When engaging any Sub-processor, the Processor shall:

- inform the Controller of all processing activities that the Sub-processor will perform for the Processor;
- ensure that the processing of personal data by the Sub-processor is governed by and carried out in accordance with these Processing Conditions, the Processing Agreement, the Instructions and Data Protection Regulations, so as to ensure an appropriate level of personal data protection. For the purpose of fulfilling the obligation under the preceding sentence, the Processor shall enter into a written agreement with the Sub-processor (hereinafter also referred to as the "***Sub-processing Agreement***"), which shall define the Sub-processor's obligations and conditions in accordance with these Processing Conditions, the Processing Agreement, the Instructions and the Data Protection Regulations, including the definition of specific technical and organisational measures;
- ensure an adequate level of protection of the Controller's personal data, including sufficient safeguards to implement appropriate technical and organisational measures in accordance with this Agreement, the Primary Agreement, the Instructions and the applicable and effective Data Protection Regulations;
- verify and regularly check that the Sub-processor processes personal data in accordance with the Sub-processing Agreement and not in breach of these Processing Conditions, the Processing Agreement, the Instructions and the Data Protection Regulations. The Controller shall inform the Processor in writing of the result of the inspection within 2 weeks of the inspection;
- In the case of transfers of personal data outside the European Economic Area, the Controller is obliged stipulate in the contracts between the Processor and the Sub-processor Standard Contractual Clauses or other mechanism approved in advance by the Controller to ensure adequate protection of the transferred personal data.

4. In the event of a breach of the Sub-processor's obligations, the Processor shall be liable to the Controller for the Sub-processor's performance of its obligations.

5. With prior written consent from the Controller, it is possible to chain processors, i.e. to conclude agreements for personal data processing between Sub-processors. Agreements concluded between Sub-processors must meet the requirements and conditions of these Processing Conditions, the Processing Agreement, the Instructions and Data Protection Regulations, so as to ensure an appropriate level of personal data protection. Without prior written consent from the Controller, the chaining of Sub-processors is excluded.

6. Processors and Sub-processors are obliged to provide the Controller with a copy of the concluded Processing/Sub-processing Agreements without undue delay, but no later than 7 days after receipt of the request.

## X. Termination of personal data processing

1. The Processor, within a reasonable period of time, and in any event no later than 45 calendar days after termination of the Primary Agreement or termination of the personal data processing for any other reason, based on written Instruction, shall either:

   a) return to the Controller a complete copy of all personal data by secure transfer of data files in the format specified in the Controller's Instruction, while securely and verifiably erasing all other copies of personal data processed by the Processor or any other Sub-processor; or

   b) securely and verifiably erase all copies of personal data processed by the Processor or any other Sub-processor.

2. The Processor shall provide the Controller with a written certificate of compliance with this article without undue delay, but no later than within 7 days.

3. Without prejudice to the obligation under paragraph 1 of this Article, the Processor shall remain entitled to process personal data to the extent required by EU or Member State law applicable to the Processor. Processing according to the previous sentence may only take place for the time, for the purpose and in accordance with the law, where the Processor is obliged to ensure, in particular, sufficient protection and confidentiality of the personal data.

## XI. Codes of Conduct and certification

1. The Processor is obliged to comply with the relevant code of conduct approved for civil air transport pursuant to Article 40 GDPR at the request of the Controller. Until the code of conduct pursuant to the preceding sentence is approved by the Office, the processor shall comply with the draft code, which is published on the Controller's website.
2. The Processor is obliged to obtain the relevant certification pursuant to Article 42 GDPR at the request of the Controller.
3. The Processor shall ensure compliance with the code of conduct or relevant parts thereof without undue delay and ensure that Sub-processors are certified.

## XII. Standard contractual clause

1. If the Processor is domiciled in a third country, the relationship between the Processor and the Controller is also governed by the so-called Standard Contractual Clause, as amended by the Annex to the Commission Decision of 5 February 2010 (notified under K (2010) 593), within the meaning of Article 26(2) of Directive 95/46/EC and Article 45(9) GDPR, whereby the Parties declare that if the Commission amends, replaces or revokes its Decision by a decision adopted pursuant to Article 45(3) or (5) GDPR, the contractual relationship will be governed by the new Commission Decision.
2. The preceding paragraph shall not apply where the Commission has decided that the third country, a particular territory or one or more specific sectors in that third country provide an adequate level of protection or where there is an international treaty by which both Parties are bound, which ensures an adequate level of protection.
3. The full text of the standard contractual clause is contained in Annex 4 to these Conditions.

## XIII. Warrant Canary

1. If the Processor is domiciled in a third country and the legislation in that country simultaneously allows a court, government or other public authorities to request the

Processor to disclose personal or non-personal data processed for the Controller, the Processor is obliged to inform the Controller of this fact without undue delay, but no later than 72 hours from the date of receipt of the request for access to such data.

## XIV. Special provisions for significant suppliers

A data Processor, who is also a significant supplier, is obliged to comply with the additional obligations set out in the following headings, which must be included in the Primary Agreement:

(a) information security provisions (in terms of confidentiality, availability and integrity),

(b) provisions on authorisation to use data,

(c) provisions on the authorship of program code or, where applicable, program licences,

(d) provisions for control and audit of the supplier (customer audit rules),

(e) provisions governing the chain of suppliers, ensuring that subcontractors undertake to comply fully with the arrangements between the obliged party and the supplier and not come into conflict with the obliged party's requirements of the supplier,

(f) provisions on the obligation of the supplier to comply with the obliged party's security policies or provisions on the approval of the supplier's security policies by the obliged party,

(g) provisions on change management,

(h) provisions on compliance of contracts with generally binding legal provisions,

(i) provisions on the supplier's obligation to inform the obliged party of

1. cyber security incidents related to the performance of the contract,

2. the supplier's risk management and residual risks associated with the performance of the contract,

3. significant changes in the control of that supplier or a change in ownership of, or authority to dispose of, the material assets used by that supplier for performance under the contract with the Controller,

(j) specification of conditions in terms of security upon termination of the contract (for example, a transition period at the end of the cooperation, when the service still needs to be maintained before deploying a new solution, data migration, etc.),

(k) specification of the conditions for business continuity management in relation to suppliers (e.g. inclusion of suppliers in contingency plans, tasks of suppliers when activating business continuity management),

(l) specification of the conditions for the format of data transfer, operational data and information upon request by the controller,

(m) rules for the disposal of data,

(n) provisions on the right to unilaterally withdraw from the contract in the event of a significant change of control of the contractor or a change of control of material assets used by the contractor for performance under the contract; and

(o) provisions on penalties for breach of obligations.

If the aforementioned areas are not addressed in the Primary Agreement between the Controller and the Processor, or in the generally binding terms and conditions of the Parties, or in the technical standards that the parties have agreed to comply with, the provisions of this Article shall apply *mutatis mutandis*. The Parties shall become familiar with and comply with the regulations summarised in the document issued by The International Air Transport Association (IATA) under the title “Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation”.

## Annex No. 1 Processing Agreement

### Agreement on Personal Data Processing

*Concluded in the year, month and day set out below in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as "GDPR") between:*

**Smartwings, a.s., ID No.: 25663135**

registered office in Prague 6, K Letišti 1068/30, 160 08, 16008

*(hereinafter also referred to as "SW CZ" or the "Controller")*

and

……*, ID No.: ……*

Registered office: ……*

Represented by: ……*

Acting through: ……*

*(hereinafter also referred to as the "Processor")*

***(the Controller and the Processor hereinafter collectively referred to as the "Parties")***

### Art. I - Introductory provisions

1. The Parties agree that the Processor, on the basis of the Agreement .....* dated .....*, performs the Service for / provides Products to the Controller (*hereinafter referred to as the* "***Primary Agreement***") and processes on behalf of the Controller the personal data of the data subjects submitted by the Controller or their demonstrably designated entity in connection with the Primary Agreement.

2. The Parties have agreed that personal data processing shall be governed by the General Conditions for the Processing of Personal Data by the Processor and Other Parties (*hereinafter referred to as the "**Processing Conditions**"*) published on the Controller's website, always according to the current version of the Processing Conditions.
3. **The Processing Conditions become a binding and inseparable part of this Processing Agreement.**
4. The Processor declares that it has read the Processing Conditions and is obliged to comply with them when processing personal data.

## Article II - Specification of personal data and processing

1. Type and nature of personal data:

   ☐ Personal data: ……

   ☐ Special category of personal data according to Article 9 GDPR:.....

2. Period of processing personal data: for the duration of the Primary Agreement. The termination of the Primary Agreement shall not affect the rights and obligations of the Processor, which by their nature or under this Agreement or the Processing Conditions are intended to survive the termination of the Primary Agreement.
3. Nature of processing:

   ☐ Processing

   ☐ Automated processing

   ☐ Profiling or automated decision-making

4. Purpose of processing: ……

5. Categories of data subjects: …….

**Art. III - Final provisions**

1. Terms used in this Agreement shall be interpreted in accordance with the Processing Conditions.
2. This Agreement comes into validity and effect upon its signing by both parties.
3. This Agreement may be altered only by written, consecutively numbered amendments and signed by both Parties. This provision is without prejudice to the possibility of amending the Processing Conditions and the granting of Instructions by the Controller to process the Controller's personal data.
4. Should any provision of this Agreement be or become invalid, this will not affect the validity of the remaining provisions hereof. The Parties to this Agreement undertake to conclude the amendment without delay to provide for new valid provisions in lieu of the invalid provisions which best correspond to the intent of the invalid provisions.
5. This Agreement is drafted in 2 counterparts with the validity of originals, of which each Party receives 1 counterpart.

In …… dated …… In …… dated ……

…… ……

Controller Processor

## Annex 2 - Technical and Organisational Measures

### 1. General provisions

The Processor is obliged to adopt binding documentation governing technical and security measures to protect and secure the processed personal data (hereinafter also referred to as the “security documentation”).

The Processor is obliged to familiarise its employees with the security documentation and these Processing Conditions and to conduct regular training.

The Processor is obliged to adapt the security documentation to the processed personal data in order to ensure an appropriate level of security.

Passwords used must meet the requirements for a very strong password, including length, character complexity and non-repeatability.

### 2. Responsible Persons and Authorised Persons

The Processor is obliged to designate specific persons responsible for ensuring and implementing technical and organisational measures, dealing with suspected personal data security breaches and a contact person for the Controller and the data subject. The Processor shall clearly define the role and responsibilities of the persons referred to in the previous sentence.

The Processor shall maintain a list of all devices on which personal data are processed. This list is updated regularly.

Authorised Persons processing personal data pursuant to Article V of these Processing Conditions have clearly defined tasks and activities in processing personal data, and process personal data only to the extent necessary to fulfil the Processor's obligations under the Primary Agreement, the Processing Agreement and these Processing Conditions.

After the termination of cooperation with the Authorised Person (e.g. termination of the main employment relationship, etc.), the Processor is obliged to ensure that no access to personal data is granted to such persons.

## 3. Access to the Processor’s premises

Access to the premises where the processing of personal data takes place (hereinafter also referred to as the “Processor's premises”) must be protected, at a minimum, by a security lock or an intrusion alarm system. It is forbidden to make the keys and codes to the alarm available to unauthorised persons. At a minimum, the following obligations must be observed when handling keys, alarm codes and access to the Processor's premises:

- Keys may not be loaned, entrusted to other persons or given as a deposit; It is forbidden to make a copy of the key without consent from the designated employee responsible for security on the Processor’s premises (hereinafter also referred to as the “*security officer*”);
- The access code is protected by confidentiality and must not be disclosed to any other person. Interception of the alarm code in any form is prohibited except for the purposes of the security officer;
- When entering the Processor's premises, it is necessary to ensure that the controlled access door is closed and that no unauthorised persons are allowed to enter the Processor's secure premises;
- The key and access code must be protected against loss, theft, misuse, destruction or damage.

At a minimum, the following principles must be observed in connection with visitors to the Processor's premises:

- Visitors cannot be left unattended anywhere where the Controller's personal data are processed;
- An unknown person on the Processor’s premises unaccompanied by a Processor's employee must be identified and accompanied to the Processor's employee whom they want to visit or handed over to the responsible person.

Allowing access to data centres, server rooms and other relevant technical rooms (hereinafter also referred to as "*technical rooms*") is subject to the approval of the

Processor's responsible employee. Visits to the technical premises must always be accompanied by a responsible employee of the Processor.

## 4. Computers and laptops

At a minimum, the following must be observed when handling computers and laptops:

- The assistance of a responsible IT employee is required for connection, disconnection and any other manipulation;
- The hard drive must be encrypted and password-protected. A password must be required when the computer and laptop system is turned on. Saving and auto-filling of the password is disabled. The password must be changed at regular intervals;
- Personal data may only be stored on the Processor's password-protected and encrypted servers, and may only be processed on encrypted and password-protected network drives and within relevant legal applications;
- The sharing of local disks, CD-ROMs, etc. is prohibited;
- The computer and laptop cannot be left unattended after switching on. In the case of temporary departure without shutting down, the computer or laptop must be locked with a password;
- Wireless technologies must be turned off by default. They can only be switched on when you need to connect to a specific network;
- The Processor may only use legally obtained software, the installation of which shall be carried out by the responsible IT employee in accordance with the relevant rules and procedures;
- The installation and distribution of illegally acquired software and text/audio/video content or its storage on a computer or laptop is prohibited;
- The computer and laptop must be protected by a firewall, antivirus and other security settings that only the responsible IT employee is authorised to activate, update and deactivate, with updates and tests taking place regularly. In case of a

suspected virus or other threat, the Processor's employee is obliged to inform the responsible IT employee immediately;

- The Processor’s employees have separate user accounts, except where necessary, in which case persons using the same user account have the same duties, tasks and responsibilities in processing personal data.

## 5. Protection of portable devices

Portable devices are mainly laptops, mobile phones, PDAs, tablets, etc.

At a minimum, the following obligations must be observed when handling portable devices:

- The portable device must be protected from access by unauthorised persons and must not be left unattended by the Processor's employees, except where this is not objectively possible;
- When being carried, the portable device must be placed within the immediate reach and control of the Processor’s employee, except where this is not objectively possible;
- In case of loss or theft of a portable device, the Processor's employee must inform the responsible person and their supervisor immediately. According to technical possibilities, the Processor is obliged to try to ensure that the portable device is blocked or erased with the help of responsible IT employees;
- The portable device must be password-protected, if objectively permitted, and the password must be required each time the portable device is used;
- The Processor's employees may not use their own portable devices to process personal data without the Processor's prior consent, where the Processor's consent may only be given in exceptional situations;
- personal data stored on portable devices may only be stored on an encrypted and password-protected storage site. Otherwise, the portable device cannot be used to store personal data;

- Tt is forbidden to connect a portable device to another device that is not under the control of the Processor (e.g. computers in internet cafes, print shops, private computers, etc.).

For cases where it is not objectively possible to protect the portable device from access by unauthorised persons, where it is not possible for it to be within the immediate reach and control of the Processor's employee, and for other cases where there is a risk of a personal data security breach, the portable device must be protected by a security cable or other secure mechanical means and at least by a password or other possible means of protection, to the fullest extent possible, so as to ensure an appropriate level of security.

For the exchange of personal data between the Processor's employees, it is necessary to use the shared storage site within the Processor's network and not to use portable media, except in exceptional and justified cases using a password and encryption, where it is necessary to permanently delete the personal data from the portable media without undue delay after the exchange.

## 6. Use of the internet, e-mail and remote access to the Processor's network

At a minimum, the following obligations must be observed when using the internet and e-mail:

- Internet access is only available through the Processor's IT infrastructure;
- The uploading and storage of personal data on public storage servers is prohibited;
- Communication over the internet is encrypted using cryptographic protocols;
- When processing personal data, only work e-mails may be used, and these may not be used for private purposes;
- Personal data transmitted via e-mail communication must be password-protected and encrypted, otherwise it cannot be transmitted in this manner;
- Automatic forwarding of e-mail messages to e-mail addresses outside the Company's network is not permitted;

- In the case of e-mail communication with more than one person, where at least one person is a person external to the Processor, it is necessary to use the hidden copy function;
- When using remote access to the Processor's local network, only the Processor's workstations or laptops and VPN connections managed by the Processor are permitted. It is forbidden to establish remote connections from other workstations that are not under the control of the Processor;
- In order to use remote access, a certificate must be assigned and installed to the Processor's employee upon prior approval by the responsible person. To log in to the VPN, the Processor's employee must identify themselves with the following information: login name, password, certificate and domain name.

## 7. Data backup and deletion of personal data

The Processor is obliged to continuously back up the personal data so that they are not destroyed, damaged or lost, etc.

When any portable device is discarded, it will first be overwritten so that the personal data are deleted. If overwriting is not possible, physical disposal will be carried out.

Any documents containing personal data to be destroyed must be shredded.

Documentation must be kept of the overwriting of equipment, shredding and disposal.

## Annex No. 3 List of Sub-processors and Transfer to Recipients in Third Countries

### 1. Transfer of personal data approved by the Controller pursuant to Article IV(4) of the Processing Conditions

| No. | Approved recipients | Registered office | Processing specifications |
|---|---|---|---|
| 1. | | | |
| 2. | | | |

### II. Approved Sub-processor pursuant to Article IX(2) of the Processing Conditions

| No. | Approved Sub-processor | Registered office | Processing specifications |
|---|---|---|---|
| 1. | | | |
| 2. | | | |

## Annex 4 Standard Contractual Clause

The personal data exporter, who is the personal data Controller pursuant to these Conditions and the Primary Agreement, and the personal data importer, who is the personal data Processor pursuant to these Conditions and the Primary Agreement, (individually referred to as the "Party" and collectively as the "Parties"), together, under the conditions of Article XII hereof, conclude the following contractual clause as part of the personal data Processing Agreement:

**DIVISION I**

***Clause 1***

**Purpose and scope of applicability**

The purpose of these standard contractual clauses is to ensure compliance with the requirements set out in 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) as regards the transfer of personal data to a third country.

Parties:

the natural person(s) or legal entity (entities), public authority or authorities, agency or agencies or other body or bodies (hereinafter referred to as the “subject” or “subjects”) transferring the personal data listed in Annex I, Part A (hereinafter referred to as the “data exporter”); and

the entity or entities in a third country receiving, directly or indirectly through another entity which is also a party to these clauses, personal data from a data exporter listed in Annex I, Part A (hereinafter referred to as the “data importer”),

have agreed to the following standard contractual clauses (hereinafter referred to as the “Clauses”).

These clauses shall apply with regard to the transfer of personal data as set out in Annex I, Part B.

The addendum to these clauses containing the annexes referred to in these clauses shall form an integral part of these clauses.

### *Clause 2*

### Effect and immutability of clauses

These clauses stipulate appropriate safeguards, including the enforceable rights of the data subject and effective legal protection, pursuant to Articles 46(1) and 46(2)(c) of Regulation (EU) 2016/679 and, with regard to transfers of data from controllers to processors and/or from processors to processors, the standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, unless amended, except for the selection of the appropriate module(s) or for the purpose of adding or updating information in the addendum. This does not prevent the Parties from including the standard contractual clauses set out in herein in a broader contract and/or adding additional clauses or additional safeguards, provided that they do not directly or indirectly conflict with these clauses or affect the fundamental rights or freedoms of data subjects.

These clauses are without prejudice to the obligations applicable to data exporters under Regulation (EU) 2016/679.

### *Clause 3*

### Authorised third parties

Data subjects may invoke and enforce these clauses as authorised third party against the exporter and/or data importer, with the following exceptions:

Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

> Clause 8 - Module 1: Clause 8.5(e) and Clause 8.9(b); Module 2: Clause 8.1(b), Clause 8.9(a), (c), (d) and (e); Module 3: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module 4: Clause 8.1(b) and Clause 8.3(b);

Clause 9 - Module 2: Clause 9(a), (c), (d) and (e); Module 3: Clause 9(a), (c), (d) and (e);

Clause 12 - Module 1: Clause 12(a) and (d); Modules 2 and 3: Clause 12(a), (d) and (f);

Clause 13;

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

Clause 16(e);

Clause 18 - Modules 1, 2 and 3: Clause 18(a) and (b); Module 4: Clause 18.

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

***Clause 4***

**Interpretation**

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

These clauses should be read and interpreted in light of the provisions of Regulation (EU) 2016/679.

These clauses will not be interpreted in any way that would conflict with the rights and obligations set out in Regulation (EU) 2016/679.

***Clause 5***

**Hierarchy**

In the event of a conflict between these clauses and the provisions of related agreements between the Parties which existed at the time of the negotiation of these clauses, or which were entered into after their negotiation, these clauses shall prevail.

*Clause 6*

**Description of transfer**

The details of transfer, in particular the categories of transferred personal data and the purpose or purposes for which they are transferred, are set out in Annex I, Part B.

*Clause 7*

**Agreement on accession**

An entity that is not a party to these clauses may, with the consent of the Parties, accede to these clauses at any time, either as a data exporter or as a data importer, by completing the addendum and signing Annex I, Part A.

Once the acceding entity completes the addendum and signs Annex I, Part A, it becomes a Party to these clauses and has the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I, Part A.

The acceding entity shall have no rights or obligations under these clauses arising from the period before it became a Party hereto.

**SECTION II - OBLIGATIONS OF THE PARTIES**

*Clause 8*

**Data protection warranties**

The data exporter warrants that it has made reasonable efforts to determine whether the data importer is able, by putting in place appropriate technical and organisational measures, to fulfil its obligations under these clauses.

**MODULE 1: Transfer from controller to controller**

**Purpose limitation**

The data importer shall only process personal data for the specific purpose or purposes of transfer in accordance with Annex I, Part B. It may process personal data for another purpose only if:

it obtained prior consent from the data subject;

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

it is necessary to protect the vital interests of the data subject or another natural person.

**Transparency**

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

of its identity and contact details;

of the categories of processed personal data;

of the right to obtain a copy of these clauses;

if it intends to transfer the personal data onward to any third party or parties, of the recipient or categories of recipients (as necessary to provide meaningful information), the purpose of such onward transfer and the reason for the onward transfer under Clause 8.7.

Letter (a) shall not apply where the data subject already has this information, even if the data exporter has already provided this information, or where it is impossible or would involve a disproportionate effort for the data importer to provide this information. In the latter case, the data importer shall disclose the information to the maximum extent possible.

The Parties shall provide the data subject, upon request and free of charge, with a copy of these clauses, including the addendum completed by the Parties. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Parties may redact part of the text of the addendum before sharing a copy, but shall provide a meaningful summary if the data subject would otherwise be unable to understand its content or exercise their rights. The parties shall, upon request, provide the data subject

with the reasons for these alterations to the greatest extent possible, without disclosing the altered information.

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

**Accuracy and data minimisation**

Each Party shall ensure that the personal data are accurate and updated where necessary. The data importer shall take all reasonable measures to ensure that personal data which are inaccurate are erased or rectified without delay, taking into account the purpose or purposes of processing.

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

The data importer shall ensure that the personal data are adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed.

**Restrictions on retention**

The data importer shall only retain the personal data for as long as necessary for the purpose or purposes for which they are processed. It shall take appropriate technical or organisational measures to ensure compliance with this obligation, including the erasure or anonymisation of data and any backups at the end of the retention period.

**Processing security**

The data importer and, during the transfer, also the data exporter shall take appropriate technical and organisational measures to ensure the security of personal data, including protection against a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access (hereinafter referred to as a "personal data security breach"). In assessing the appropriate level of security, due account shall be taken of technical progress, cost of implementation, the nature, scope, context and purpose

or purposes of processing, and the risks to the data subject associated with processing. In particular, the Parties shall consider the use of encryption or pseudonymisation, including during transmission, if the purpose of the processing can be fulfilled in this manner.

The Parties agree on the technical and organisational measures set out in Annex II. The data importer conducts out regular checks to ensure that these measures still provide an adequate level of security.

The data importer shall ensure that the persons authorised to process personal data undertake to observe confidentiality or are subject to a legal nondisclosure obligation.

In the event of a personal data security breach involving personal data processed by the data importer under these clauses, the data importer shall take appropriate measures to address the personal data security breach, including measures to mitigate its potential adverse effects.

In the event of a personal data breach that could lead to a threat to the rights and freedoms of natural persons, the data importer shall inform the data exporter and the competent supervisory authority without undue delay in accordance with Clause 13. This notification shall include i) a description of the nature of the personal data security breach (including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned), ii) its likely consequences, iii) a description of the measures taken or proposed to address the security breach, and iv) information about the point of contact where additional information can be obtained. If the data importer cannot provide all the information simultaneously, it may be provided gradually without further undue delay.

In the event of a personal data security breach that is likely to pose a high risk to the rights and freedoms of natural persons, the data importer shall also, without undue delay, notify

the data subjects concerned of the personal data breach and its nature, in cooperation with the data exporter if necessary, and shall also provide them with the information referred to in letter (e)(ii) to (iv), unless the data importer has implemented measures to substantially reduce the risk to the rights and freedoms of natural persons or if the notification requires disproportionate effort. In the latter case, the data importer shall instead issue a public notice or ensure a similar measure to inform the public of the personal data security breach.

The data importer shall document and keep a record of all relevant facts relating to the personal data security breach, including its consequences and the corrective measures taken.

**Sensitive data**

If 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 the health or sex life or sexual orientation of a natural person, or data concerning criminal convictions or offences (hereinafter referred to as “sensitive data”), the data importer shall apply the specific limitations and/or additional safeguards adapted to the special nature of the data and the related risks. This may include restrictions on the employees permitted to access personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to onward disclosure.

**Onward transfer**

The data importer shall not disclose personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter referred to as “onward transfer”) unless that third party is bound by or agrees to be bound by these clauses under the relevant module. Onward transfer by the data importer may otherwise only take place with the consent of the Controller and only if:

it is made to a country that makes use of an adequacy decision under Article 45 of Regulation (EU) 2016/679, which governs onward transfers;

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

the third party concluded 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 warranties to the data exporter;

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

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

if none of the other conditions apply, the data importer has obtained the data subject's explicit consent to onward transfer in the specific situation, after informing the data subject of the purpose or purposes of the transfer, the identity of the recipient and the possible risks of such transfer to the data subject due to the lack of appropriate data protection safeguards. In such case, the data importer shall inform the data exporter and, at the request of the data exporter, provide the data exporter with a copy of the information provided to the data subject.

Any onward transfer is subject to the condition that the data importer complies with all other safeguards under these clauses, in particular purpose limitation.

**Processing on behalf of the data importer**

The data importer shall ensure that any person acting on its behalf, including the Processor, processes the data only on its instructions.

**Documentation and compliance**

Each Party must be able to demonstrate compliance with its obligations under these clauses. In particular, the data importer shall keep appropriate documentation of the processing activities for which it is responsible.

The data importer shall make this documentation available to the competent supervisory authority upon request.

**MODULE 2: Transfer from controller to processor**

**Instructions**

The data importer processes personal data only on the basis of documented instructions from the data exporter. The data exporter may issue such instructions throughout the duration of the agreement.

The data importer shall inform the data exporter immediately if it is unable to comply with these instructions.

**Purpose limitation**

The data importer shall only process personal data for the specific purpose or purposes of the transfer listed in Annex I, Part B, unless the data exporter issues further instructions.

**Transparency**

Upon request, the data exporter shall provide a copy of these clauses, including the addendum completed by the parties, to the data subject free of charge. To the extent necessary to protect trade 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 addendum to these clauses before sharing a copy, but shall provide a meaningful summary if the data subject would otherwise be unable to understand its content or exercise their rights. The parties shall, upon request, provide the data subject with the reasons for these alterations to the greatest extent possible, without disclosing the altered information. This

clause is without prejudice to the data exporter's obligations under Articles 13 and 14 of Regulation (EU) 2016/679.

**Accuracy**

If the data importer becomes aware that the personal data it has received are inaccurate or outdated, it shall inform the data exporter without undue delay. In such a case, the data importer shall cooperate with the data exporter to correct or delete the data.

**Processing time and erasure or return of data**

The data importer shall only process the data for the period specified in Annex I, Part B. Upon termination of the provision of processing services, the data importer shall, in accordance with the data exporter's choice, erase all personal data processed on behalf of the data exporter and confirm to the data exporter that it has done so, or return all personal data processed on its behalf to the data exporter and erase any existing copies. Until the data are deleted or returned, the data importer shall continue to ensure compliance with these clauses. If the data importer is subject to local legal regulations that prohibit it from returning or erasing personal data, the data importer warrants that it will continue to ensure compliance with these clauses and that it will only process data to the extent and for as long as required by local law. This is without prejudice to Clause 14, in particular the requirement under Clause 14(e) for the data importer to inform the data exporter throughout the duration of the agreement, if it has reason to believe that it is or has become subject to legal regulations or procedures which do not comply with the requirements under Clause 14(a).

**Processing security**

The data importer and, during the transfer, also the data exporter shall take appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to that data (hereinafter referred to as a "personal data security breach"). In assessing the appropriate level of security, due account

shall be taken of technical progress, cost of implementation, the nature, scope, context and purpose or purposes of processing, and the risks to the data subject associated with processing. In particular, the Parties shall consider the use of encryption or pseudonymisation, including during transmission, if the purpose of the processing can be fulfilled in this manner. In the case of pseudonymisation, the additional information for the attribution of personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In order to comply with its obligations under this paragraph, the data importer must at least implement the technical and organisational measures set out in Annex II. The data importer conducts out regular checks to ensure that these measures still provide an adequate level of security.

The data importer shall only provide access to the personal data to its employees to the extent necessary for the implementation, administration and monitoring of the agreement. It shall ensure that the persons authorised to process personal data undertake to observe confidentiality or are subject to a legal nondisclosure obligation.

In the event of a personal data security breach involving 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 report to the data exporter without undue delay after becoming aware of the breach. Such notification shall include details of a point of contact that can provide further information, a description of the nature of the security breach (including, where possible, the categories and approximate number of data subjects concerned and the approximate number of personal data records), its likely consequences and the measures taken or proposed to address the security breach, including any measures to mitigate its possible adverse effects. If it is not possible to provide all the information at the same time, the initial report shall contain the information that was available at the time and further information, as it becomes available, shall be provided without undue delay thereafter.

The data importer shall cooperate with and assist the data exporter to enable it to fulfil its obligations under Regulation (EU) 2016/679, in particular the obligation to report to the

competent supervisory authority and the data subjects concerned, taking into account the nature of processing and the information available to the data importer.

**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 the health or sex life or sexual orientation of a natural person, or data concerning criminal convictions and offences (hereinafter referred to as "sensitive data"), the data importer shall apply the specific limitations and/or additional safeguards described in Annex I, Part B.

**Onward transfer**

The data importer shall only disclose personal data to a third party on the basis of documented instructions from the data exporter. Additionally, the data may be disclosed to a third party domiciled outside the European Union (in the same country as the data importer or in another third country, hereinafter referred to as "onward transfer") if that third party is bound by or agrees to be bound by these clauses under the relevant module, or if:

onward transfer is made to a country that makes use of an adequacy decision under Article 45 of Regulation (EU) 2016/679, which governs onward transfers;

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

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

onward transfer is necessary to protect the vital interests of the data subject or another natural person.

Any onward transfer is subject to the condition that the data importer complies with all other safeguards under these clauses, in particular purpose limitation.

**Documentation and compliance**

The data importer shall deal promptly and appropriately with enquiries from the data exporter concerning processing under these clauses.

The Parties must be able to demonstrate compliance with these clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out on behalf of the data exporter.

The data importer shall provide the data exporter with all information necessary to demonstrate that the obligations stipulated in these clauses have been complied with and shall, at the request of the data exporter, facilitate and contribute to audits of the processing activities covered by these clauses at reasonable intervals or where there are circumstances indicating that the clauses are not being complied with. When deciding on a review or audit, the data exporter may take into account the relevant certificates held by the data importer.

The data exporter may decide to conduct the audit itself or to commission an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and, where appropriate, shall be carried out on reasonably timely notice.

The Parties shall, upon request, provide the competent supervisory authority with the information referred to in points (b) and (c), including the results of any audits.

MODULE 3: Transfer from Processor to Processor

**Instructions**

The data exporter has informed the data importer that it is acting as a Processor on the basis of instructions from its Controller or Controllers, and the data exporter will make those instructions of available to the data importer before processing.

The data importer shall only process personal data on the basis of documented instructions from the Controller that have been communicated by the data exporter to the data importer, and on the basis of any additional documented instructions from the data exporter. These additional instructions must not be contrary to the instructions of the Controller. The Controller or data exporter may issue further documented instructions regarding the processing of the data during the duration of the agreement.

The data importer shall inform the data exporter immediately if it is unable to comply with these instructions. If the data importer is unable to follow the Controller's instructions, the data exporter shall inform the Controller without delay.

The data exporter shall ensure that it has imposed on the data importer the same data protection obligations as those stipulated in the agreement or other legal act under Union or Member State law between the data Controller and the data exporter.

**Purpose limitation**

The data importer shall only process personal data for the specific purpose or purposes of transfer in accordance with Annex I, Part B, unless there are further instructions from the Controller communicated to the data importer by the data exporter or further instructions from the data exporter.

**Transparency**

Upon request, the data exporter shall provide a copy of these clauses, including the addendum completed by the parties, to the data subject free of charge. To the extent necessary to protect trade secrets or other confidential information, including personal data, the data exporter may redact part of the text of the addendum before sharing a copy, but shall provide a meaningful summary if the data subject would otherwise be unable to understand its content or exercise their rights. The parties shall, upon request, provide the data subject with the reasons for these alterations to the greatest extent possible, without disclosing the altered information.

**Accuracy**

If the data importer becomes aware that the personal data it has received are inaccurate or outdated, it shall inform the data exporter without undue delay. In such a case, the data importer shall cooperate with the data exporter to correct or delete the data.

**Processing time and erasure or return of data**

The data importer shall only process the data for the period specified in Annex I, Part B. Upon termination of the provision of processing services, the data importer shall, in accordance with the data exporter's choice, erase all personal data processed on behalf of the Controller and confirm to the data exporter that it has done so, or return all personal data processed on its behalf to the data exporter and erase all existing copies. Until the data are deleted or returned, the data importer shall continue to ensure compliance with these clauses. If the data importer is subject to local legal regulations that prohibit it from returning or erasing personal data, the data importer warrants that it will continue to ensure compliance with these clauses and that it will only process data to the extent and for as long as required by local law. This is without prejudice to Clause 14, in particular the requirement under Clause 14(e) for the data importer to inform the data exporter throughout the duration of the agreement, if it has reason to believe that it is or has become subject to legal regulations or procedures which do not comply with the requirements under Clause 14(a).

**Processing security**

The data importer and, during the transfer, also the data exporter shall take appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to that data (hereinafter referred to as a "personal data security breach"). In assessing the appropriate level of security, due account shall be taken of technical progress, cost of implementation, the nature, scope, context and purpose or purposes of processing, and the risks to the data subject associated with processing. In particular, the Parties shall consider the use of encryption or pseudonymisation, including during transmission, if the purpose of the processing can be fulfilled in this manner. In the case of pseudonymisation, the additional information for the attribution of personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or Controller. In order to comply with its obligations under this paragraph, the data importer must at least implement the technical and organisational measures set out in Annex II. The data importer conducts out regular checks to ensure that these measures still provide an adequate level of security.

The data importer shall only provide access to the data to its employees to the extent necessary for the implementation, administration and monitoring of the agreement. It shall ensure that the persons authorised to process personal data undertake to observe confidentiality or are subject to a legal nondisclosure obligation.

In the event of a personal data security breach involving 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 report to the data exporter and, where appropriate and practicable, to the Controller without undue delay after becoming aware of the breach. Such notification shall include details of a point of contact that can provide further information, a description of the nature of the security breach (including, where possible, the categories and approximate number of data subjects concerned and the approximate number of personal data records), its likely consequences and the measures taken or proposed to address the data security breach, including measures to mitigate its possible adverse effects. If it is not possible to provide all

the information at the same time, the initial report shall contain the information that was available at the time and further information, as it becomes available, shall be provided without undue delay thereafter.

The data importer shall cooperate with and assist the data exporter to enable it to fulfil its obligations under Regulation (EU) 2016/679, in particular the obligation to report to its Controller so that the Controller can inform the competent supervisory authority and the data subjects concerned, taking into account the nature of processing and the information available to the data importer.

**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 the health or sex life or sexual orientation of a natural person, or data concerning criminal convictions and offences (hereinafter referred to as “sensitive data”), the data importer shall apply the specific limitations and/or additional safeguards stipulated in Annex I, Part B.

**Onward transfer**

The data importer shall only disclose personal data to a third party on the basis of documented instructions from the Controller, which have been communicated to the data importer by the data exporter. Additionally, the data may be disclosed to a third party domiciled outside the European Union (in the same country as the data importer or in another third country, hereinafter referred to as “onward transfer”) if that third party is bound by or agrees to be bound by these clauses under the relevant module, or if:

onward transfer is made to a country that makes use of an adequacy decision under Article 45 of Regulation (EU) 2016/679, which governs onward transfers;

the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

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

onward transfer is necessary to protect the vital interests of the data subject or another natural person.

Any onward transfer is subject to the condition that the data importer complies with all other safeguards under these clauses, in particular purpose limitation.

**Documentation and compliance**

The data importer shall deal promptly and appropriately with enquiries from the data exporter or Controller concerning processing under these clauses.

The Parties must be able to demonstrate compliance with these clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out on behalf of the Controller.

The data importer shall provide the data exporter with all information necessary to demonstrate compliance with the obligations set out in these clauses, which the data exporter shall then provide to the Controller.

The data importer shall facilitate and contribute to audits by the data exporter concerning the processing activities covered by these clauses at reasonable intervals or where there are circumstances indicating that the clauses are not being complied with. The same applies if the data exporter requests an audit on the basis of instructions from the Controller. When

deciding on the audit, the data exporter may take into account the relevant certificates held by the data importer.

If the audit is carried out on the basis of instructions from the Controller, the Controller will be informed of the results by the data exporter.

The data exporter may decide to conduct the audit itself or to commission an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and, where appropriate, shall be carried out on reasonably timely notice.

The Parties shall, upon request, provide the competent supervisory authority with the information referred to in points (b) and (c), including the results of any audits.

**MODULE 4: Transfer from Processor to Controller**

**Instructions**

The data exporter processes personal data only on the basis of documented instructions from the data importer, who acts as its Controller.

The data exporter shall inform the data importer immediately if it is unable to comply with these guidelines, including where these guidelines infringe Regulation (EU) 2016/679 or other Union or Member State data protection legislation.

The data importer shall refrain from taking any measures that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or where cooperation with the competent supervisory authorities is involved.

Upon termination of the provision of processing services, the data exporter shall, in accordance with the data importer's choice, erase all personal data processed on behalf of the data importer and confirm to the data importer that it has done so, or return all personal data processed on its behalf to the data importer and erase all existing copies.

**Processing security**

The Parties shall put in place appropriate technical and organisational measures to ensure the security of data, including during transfer, and to ensure protection against security breaches resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter referred to as a "personal data security breach"). In assessing the appropriate level of security, the Parties shall take due account of technical progress, cost of implementation, the nature of the personal data, the nature, scope, context and purpose or purposes of processing, and the risks to data subjects associated with the processing, and in particular shall consider the use of encryption or pseudonymisation, including during transfer, if the purpose of the processing can be fulfilled in this way.

The data exporter shall assist the data importer in ensuring adequate data security in accordance with letter (a). In the event of a personal data breach relating to personal data processed by the data exporter under these clauses, the data exporter shall report the breach to the data importer without undue delay after becoming aware of it and shall assist the data importer in resolving the breach.

The data exporter shall ensure that the persons authorised to process personal data undertake to observe confidentiality or are subject to a legal nondisclosure obligation.

**Documentation and compliance**

The Parties must be able to demonstrate compliance with these clauses.

The data exporter shall provide the data importer with all the information necessary to demonstrate that the obligations set out in these clauses have been met and shall facilitate and contribute to audits.

*Clause 9*

**Use of Sub-processors**

**MODULE 2: Transfer from Controller to Processor**

OPTION 1: SPECIAL PRIOR AUTHORISATION The data importer shall not subcontract any of its processing activities carried out on behalf of the data exporter under these clauses to a sub-processor without the prior specific written authorization of the data exporter. The data importer shall submit a request for specific authorisation at least 60 days before engaging the sub-processor, together with the information necessary for the data exporter to decide on the authorisation. The list of sub-processors that have already obtained a data exporter authorisation is set out in Annex III. The Parties shall update Annex III on an ongoing basis.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has general authorisation from the data exporter to engage the sub-processor or sub-processors on the approved list. The data importer shall explicitly inform the data exporter in writing of any intended changes to that list consisting in the addition or replacement of sub-processors at least 60 days in advance, thereby allowing the data exporter sufficient time to object to such changes before the sub-processor or sub-processors are engaged. The data importer shall provide the data exporter with the information necessary for the data exporter to exercise its right to object.

Where the data importer engages a sub-processor (on behalf of the data exporter) to carry out specific processing activities, it does so by means of a written agreement which, in principle, stipulates the same data protection obligations as those binding on the data importer under these clauses, including as regards the rights of the authorised third party in the case of data subjects. The Parties agree that by complying with this clause, the data importer is fulfilling its obligations under Clause 8.8. The data importer shall ensure that the

sub-processor complies with the obligations that apply to data importers in accordance with these clauses.

The data importer shall provide the data exporter, upon request, with a copy of such agreement with the sub-processor and any subsequent amendments thereto. To the extent necessary to protect trade secrets or other confidential information, including personal data, the data importer may modify the text of this Agreement before sharing a copy.

The data importer remains fully liable to the data exporter for the fulfilment of the obligations of the sub-processor on the basis of the agreement it has concluded with the data importer. The data importer shall inform the data exporter of any case where the sub-processor has failed to fulfil its obligation under the agreement.

The data importer shall negotiate a clause with the sub-processor in favour of an authorised third party, whereas - in the event that the data importer has effectively disappeared, legally dissolved or become insolvent - the data exporter shall have the right to terminate the agreement with the sub-processor and instruct the sub-processor to erase or return the personal data.

**MODULE 3: Transfer from Processor to Processor**

OPTION 1: SPECIAL PRIOR AUTHORISATION The data importer shall not subcontract any of its processing activities carried out on behalf of the data exporter under these clauses to a sub-processor without the prior specific written authorization of the Controller. The data importer shall submit a request for specific authorisation at least 60 days before engaging the sub-processor, together with the information necessary for the Controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors that have already obtained a Controller authorisation is set out in Annex III. The Parties shall update Annex III on an ongoing basis.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has general authorisation from the Controller to engage the sub-processor or sub-processors on the approved list. The data importer shall explicitly inform the Controller in writing of any intended changes to that list consisting in the addition or replacement of sub-processors at least 60 days in advance, thereby allowing the Controller sufficient time to object to such changes before the sub-processor or sub-processors are engaged. The data importer shall provide the Controller with the information necessary for the Controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

Where the data importer engages a sub-processor (on behalf of the Controller) to carry out specific processing activities, it does so by means of a written agreement which, in principle, stipulates the same data protection obligations as those binding on the data importer under these clauses, including as regards the rights of the authorised third party in the case of data subjects. The Parties agree that by complying with this clause, the data importer is fulfilling its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations that apply to data importers in accordance with these clauses.

The data importer shall provide the data exporter or Controller, upon their request, with a copy of such agreement with the sub-processor and any subsequent amendments thereto. To the extent necessary to protect trade secrets or other confidential information, including personal data, the data importer may modify the text of this Agreement before sharing a copy.

The data importer remains fully liable to the data exporter for the fulfilment of the obligations of the sub-processor on the basis of the agreement it has concluded with the data importer. The data importer shall inform the data exporter of any case where the sub-processor has failed to fulfil its obligation under the agreement.

The data importer shall negotiate a clause with the sub-processor in favour of an authorised third party, whereas - in the event that the data importer has effectively disappeared, legally

dissolved or become insolvent - the data exporter shall have the right to terminate the agreement with the sub-processor and instruct the sub-processor to erase or return the personal data.

***Clause 10***

**Rights of data subjects**

**MODULE 1: Transfer from Controller to Controller**

The data importer, with the assistance of the data exporter where applicable, shall deal with all enquiries and requests it receives from the data subject concerning the processing of their personal data and the exercise of their rights under these clauses without undue delay and within one month of receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate the handling of such enquiries, requests and the exercise of the data subject's rights. All information provided to the data subject shall be in a comprehensible and easily accessible form using clear and plain language.

At the request of the data subject, the data importer shall, in particular and free of charge:

to provide the data subject with confirmation as to whether personal data relating to them are being processed and, if so, provide them with a copy of the data relating to them and the information set out in Annex I; where personal data have been or will be transferred onward, to provide information about the recipients or categories of recipients (as necessary to provide meaningful information) to which the personal data have been or will be transferred onward, the purpose of such onward transfers and the reason for them in accordance with Clause 8.7; and provide information on the right to lodge a complaint with the supervisory authority in accordance with Clause 12(c)(i);

to correct inaccurate or incomplete data concerning the data subject;

to erase personal data relating to the data subject if the data are or have been processed in breach of any of these clauses safeguarding the rights of the authorised third party, or if the data subject withdraws the consent on which the processing is based.

Where the data importer processes personal data for direct marketing purposes, it shall cease to process them for those purposes if the data subject objects.

The data importer shall not take a decision based solely on the automated processing of transferred personal data (hereinafter referred to as an “automated decision”) which would have legal effects concerning the data subject or similarly significantly affect them, unless the data subject has given their explicit consent or unless it is permitted to do so under the legal regulations of the country of destination, provided that such legal regulations stipulate appropriate measures to protect the rights and legitimate interests of the data subject. In this case, the data importer, in cooperation with the data exporter, if necessary :

shall inform the data subject of the envisaged automated decision, the envisaged consequences and the procedure to be followed; and

shall put in place appropriate safeguards, at least by allowing the data subject to challenge the decision, express their views and obtain a human review.

Where requests from the data subject are excessive, in particular because they are repetitive, the data importer may either impose a reasonable fee, taking into account the administrative costs involved in complying with the request, or refuse to comply with the request.

The data importer may refuse the data subject's request where such refusal is permitted under the legal regulations of the country of destination and is necessary and proportionate

in a democratic society in order to protect one of the purposes referred to in Article 23(1) of Regulation (EU) 2016/679.

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

**MODULE 2: Transfer from Controller to Processor**

The data importer shall inform the data exporter without delay of any request received from the data subject. It will not respond to this request itself unless it has received permission to do so from the data exporter.

The data importer shall assist the data exporter in fulfilling its obligations to respond to requests from data subjects concerning the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall stipulate in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing through which assistance will be provided, and the scope and extent of the assistance required.

In carrying out its obligations under letters (a) and (b), the data importer must comply with the instructions of the data exporter.

**MODULE 3: Transfer from Processor to Processor**

The data importer shall inform the data exporter and, where applicable, the Controller without delay of any request received from the data subject, without responding to the request, unless it has been authorised to do so by the controller.

The data importer, in cooperation with the data exporter where appropriate, shall assist the Controller in fulfilling its obligations to respond to requests from data subjects concerning the exercise of their rights under Regulation (EU) 2016/679 or, where applicable, Regulation

(EU) 2018/1725. In this regard, the Parties shall stipulate in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing through which assistance will be provided, and the scope and extent of the assistance required.

In carrying out its obligations under letters (a) and (b), the data importer must comply with the instructions of the Controller, disclosed to it by the data exporter.

**MODULE 4: Transfer from Processor to Controller**

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

***Clause 11***

**Rectification**

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

[VARIANT: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body free of charge (11). The data importer shall inform the data subjects of this redress mechanism and of the fact that data subjects are not obliged to make use of it or to follow a specific procedure for seeking redress in the manner referred to in letter (a).]

**MODULE 1: Transfer from Controller to Controller**

**MODULE 2: Transfer from Controller to Processor**

**MODULE 3: Transfer from Processor to Processor**

In the event of a dispute between a data subject and one of the Parties regarding compliance with these clauses, that Party shall use its best efforts to resolve the matter amicably and in a timely manner. The Parties shall inform each other of such disputes and, where appropriate, cooperate in resolving them.

If the data subject invokes the right in favour of an authorised third party under Clause 3, the data importer shall accept the data subject's decision:

to lodge a complaint with the supervisory authority in the Member State of their usual residence or place of work or with the competent supervisory authority under clause 13;

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

The Parties acknowledge that the data subject may be represented by a non-profit entity, organisation or association under the conditions stipulated in Article 80(1) of Regulation (EU) 2016/679.

The data importer complies with a decision binding under applicable EU or Member State law.

The data importer agrees that the choice made by the data subject shall not affect their substantive and procedural rights to seek redress in accordance with applicable law.

***Clause 12***

**Liability**

**MODULE 1: Transfer from Controller to Controller MODULE 4: Transfer from Processor to Controller**

Each Party shall be liable to the other Party/other parties for any damage caused to the other Party/other parties by its breach of these clauses.

Each party is liable to the data subject, and the data subject is entitled to compensation for any tangible or intangible damage caused to the data subject by a Party's infringement of the rights of the authorised third party under these clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

Where more than one Party is responsible for the 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 authorised to bring an action against any of these Parties in court.

The Parties agree that if one of the Parties is liable pursuant to letter (c), it is authorised to recover from the other Party (Parties) a portion of the compensation corresponding to its liability for damages.

The data importer cannot appeal on the grounds of the conduct of the Processor or Sub-processor to avoid its own liability.

**MODULE 2: Transfer from Controller to Processor**

**MODULE 3: Transfer from Processor to Processor**

Each Party shall be liable to the other Party/other parties for any damage caused to the other Party/other parties by its breach of these clauses.

The data importer is liable to the data subject, and the data subject is entitled to compensation for any tangible or intangible damage caused to the data subject by the data importer's or its Sub-processor's infringement of the rights of the authorised third party under these clauses.

Without prejudice to letter (b), the data exporter is liable to the data subject, and the data subject is entitled to compensation for any tangible or intangible damage caused to the data subject by the data exporter's or data importer's (or its Sub-processor's) infringement of the rights of the authorised third party 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 the Controller, the Controller's liability under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

The Parties agree that if the data exporter is liable under letter (c) for damage caused by the data importer (or its Sub-processor), it is authorised to claim from the data importer a portion of the compensation for damages corresponding to the data importer's liability for damages.

If more than one Party is liable for the damage caused to the data subject as a result of a breach of these clauses, all liable Parties shall be jointly and severally liable and the data subject is authorised to bring an action against any of these Parties in court.

The Parties agree that if one of the Parties is liable pursuant to letter (e), it is authorised to recover from the other Party (Parties) a portion of the compensation corresponding to its liability for damages.

The data importer cannot appeal on the grounds of the conduct of its Sub-processor to avoid its own liability.

*Clause 13*

**Supervision**

**MODULE 1: Transfer from Controller to Controller MODULE 2: Transfer from Controller to Processor**

**MODULE 3: Transfer from Processor to Processor**

[Where the data exporter is domiciled in an EU Member State:] The supervisory authority specified in Annex I, Part C, which is responsible for ensuring that the data exporter complies with Regulation (EU) 2016/679 as regards the transfer of data, shall act as the competent supervisory authority.

[Where the data exporter is not domiciled in an EU Member State but falls within the territorial scope of Regulation (EU) 2016/679 in accordance with Article 3(2) thereof and has appointed a representative in accordance with Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State - specified in Annex I, Part C-, in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is domiciled, shall act as the competent supervisory authority.

[Where the data exporter is not domiciled in an EU Member State but falls within the territorial scope of Regulation (EU) 2016/679 in accordance with Article 3(2) thereof, but without 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 are transferred under these clauses in relation to goods or services offered to them or whose behaviour is monitored, as listed in Annex I, Part C, are located, shall act as the competent supervisory authority.

The data importer agrees to submit to the jurisdiction of the competent supervisory authority and to cooperate with it in all procedures aimed at ensuring compliance with these clauses. In particular, the data importer agrees to respond to inquiries, to submit to audits and to comply with the measures taken by the supervisory authority, including corrective and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary measures have been taken.

## SECTION III - LOCAL LEGISLATION AND OBLIGATIONS IN THE CASE OF ACCESS BY PUBLIC AUTHORITIES

### *Clause 14*

### Local legal regulations and procedures affecting compliance with the clauses

**MODULE 1: Transfer from Controller to Controller**

**MODULE 2: Transfer from Controller to Processor**

**MODULE 3: Transfer from Processor to Processor**

**MODULE 4: Transfers from processor to controller** *(if the EU processor combines personal data received from a controller in a third country with personal data collected by the EU processor)*

The Parties guarantee that they have no reason to believe that the legal regulations and procedures in the third country of destination that apply to personal data processing by the data importer, including any disclosure requirements or measures permitting access by public authorities, prevent the data importer from fulfilling its obligations under these clauses. This is based on the assumption that legal regulations and procedures which respect the essence of fundamental rights and freedoms and do not go beyond what is necessary

and proportionate in a democratic society to ensure one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, do not contravene these clauses.

The Parties declare that they have taken due account of the following elements in particular when providing the guarantee referred to in letter (a):

the specific circumstances of transfer, including the length of the processing chain, the number of entities involved, and the data transmission channels used, the intended onward transfer, the type of recipient, the purposes of the processing, the category and format of transferred personal data, the economic sector in which the transfer takes place, the place where the data transferred are stored;

the legal regulations and procedures of the third country of destination - including those requiring disclosure to, or allowing access by, public authorities - relevant to the specific circumstances of the transfer, as well as applicable limitations and safeguards (12);

any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these clauses, including measures applied during the transfer and processing of personal data in the country of destination.

The data importer warrants that it has made its best efforts to provide the data exporter with relevant information when carrying out the assessment under letter (b) and agrees to continue to cooperate with the data exporter in ensuring compliance with these clauses.

The Parties agree to document the assessment under letter (b) and make it available to the relevant supervisory authority upon request.

The data importer agrees to notify the data exporter without delay if, after consenting to these provisions and for the duration of the contract, it has reason to believe that it is subject to, or has become subject to, legal regulations or procedures that do not comply with the requirements referred to in letter (a), even after a change in the third country's legal regulations or measures (such as a data disclosure request), which indicates that the application of such legal regulations in practice does not comply with the requirements referred to in letter (a): [Regarding Module 3: The data exporter shall forward the report to the controller.]

Following the notice under letter (e), or where 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 taken by the data exporter and/or the data importer to address the situation [as regards Module 3: in consultation with the Controller, as appropriate]. The data exporter shall suspend the data transfer if it believes that no appropriate safeguards can be provided for the transfer or if instructed to do so by [in respect of Module 3: the Controller or] the competent supervisory authority. In this case, the data exporter is authorised to terminate the agreement with regard to the processing of personal data under these clauses. If the agreement involves more than two parties, the data exporter may exercise this right of termination only in relation to the relevant party, unless the parties have agreed otherwise. If the agreement is terminated under this clause, Clause 16(d) and (e) shall apply.

***Clause 15***

**Obligation of the data importer in case of access by public authorities**

**MODULE 1: Transfer from Controller to Controller**

**MODULE 2: Transfer from Controller to Processor**

**MODULE 3: Transfer from Processor to Processor**

**MODULE 4: Transfers from processor to controller** *(if the EU processor combines personal data received from a controller in a third country with personal data collected by the EU processor)*

**Notice**

The data importer agrees to notify the data exporter and, where possible, the data subject (with the assistance of the data exporter, if necessary) immediately if:

under the legal regulations of the country of destination, it receives a legally binding request from a public authority, including judicial authorities, for disclosure of personal data transferred under these clauses; such notice shall include information about the requested personal data, the requesting authority, the legal grounds for the request and the response given; or

it becomes aware of any direct access by public authorities to personal data transferred under these clauses in accordance with the legal regulations of the country of destination; such notice shall include all information available to the importer.

[Regarding Module 3: The data exporter shall forward the report to the controller.]

Where the data importer is prohibited under the legal regulations of the country of destination from informing the data exporter and/or the data subject, the data importer agrees to use its best efforts to waive this prohibition in order to communicate as much information as possible as quickly as possible. The data importer agrees to document its best efforts to demonstrate them upon request by the data exporter.

If permitted by the legislation of the country of destination, the data importer agrees to provide the data exporter with the most relevant information on the requests received at regular intervals throughout the duration of the agreement (in particular information about the number of requests, the type of data requested, the requesting authority or authorities, whether such requests have been challenged and the outcome of such challenge, etc.). [Regarding Module 3: The data exporter shall forward the information to the Controller.]

The data importer agrees to keep the information referred to in letters (a) to (c) for the duration of the agreement and to provide it to the competent supervisory authority upon request.

Letters (a) to (c) are without prejudice to the data importer's obligation under Clause 14(e) and Clause 16 to inform the data exporter without delay if it is unable to comply with those clauses.

**Legality review and data minimisation**

The data importer agrees to examine the lawfulness of the request for data, in particular whether it has exceeded the limits of the powers conferred on the requesting public authority, and to contest the request if, after careful consideration, it concludes that there are reasonable grounds to believe that the request is unlawful under the legal regulations of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall make use of the possibility of appeal under the same conditions. When challenging the request, the data importer shall take interim measures to suspend the effects of the request until the competent judicial authority has ruled on its merits. It will not disclose the requested personal data until it is obliged to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

The data importer agrees to document its legal assessment and any challenge to the data request and, to the extent permitted by the legal regulations of the country of destination, to make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [Regarding Module 3: The data exporter shall make the assessment available to the Controller.]

The data importer agrees to provide the minimum permissible amount of information in response to a disclosure request, based on a reasonable interpretation of the request.

## DIVISION IV - FINAL PROVISIONS

### *Clause 16*

### Failure to comply with clauses and termination

The data importer shall immediately inform the data exporter if it is unable to comply with these clauses for any reason.

If the data importer breaches these clauses or is unable to comply with them, the data exporter shall suspend the transfer of personal data to the data importer until compliance is regained or the agreement is terminated. This is without prejudice to Clause 14(f).

The data exporter is authorised to terminate the agreement to the extent to which personal data is processed under these clauses if:

the data exporter has suspended the transfer of personal data to the data importer pursuant to letter (b), and compliance with those clauses is not regained within a reasonable period, and in any event within one month of the suspension;

the data importer materially or persistently breaches these clauses; or

the data importer fails to comply with a binding decision of a competent court or supervisory authority concerning its obligations under these clauses.

In such cases, it shall inform the relevant supervisory authority [regarding Module 3: and the Controller] of such non-compliance. If the agreement involves more than two parties, the data exporter may exercise this right of termination only in relation to the relevant party, unless the parties have agreed otherwise.

[In the case of Module 1, 2 and 3: Personal data that have been transferred before the termination of the agreement pursuant to letter (c) shall, at the data exporter's discretion, be returned to the data exporter without delay or deleted in their entirety. The same shall apply in relation to any copies of the data.] [regarding Module 4: Personal data collected by the data exporter in the EU, which were transferred before the termination of the agreement under letter (c) must be erased in their entirety, including any copies thereof, without delay.] The data importer shall confirm to the data exporter that the data have been erased. Until the data are deleted or returned, the data importer shall continue to ensure compliance with these clauses. If the data importer is subject to local legal regulations that prohibit it from returning or erasing the transferred personal data, the data importer warrants that it will continue to ensure compliance with these clauses and that it will only process data to the extent and for as long as required by the said local law.

Either party may withdraw its consent to be bound by these clauses if (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 concerning the transfer of personal data covered by these clauses, or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data are transferred. This is without prejudice to other obligations applicable to the processing in question under Regulation (EU) 2016/679.

***Clause 17***

**Applicable law**

**MODULE 1: Transfer from Controller to Controller**

**MODULE 2: Transfer from Controller to Processor**

**MODULE 3: Transfer from Processor to Processor**

[VARIANT 1 These clauses are governed by the law of an EU Member State, provided that such law allows the exercise of rights belonging to the authorised third party. The Parties agree to be governed by the law of the *personal data exporter*.]

[VARIANT 2 (regarding modules 2 and 3): These clauses are governed by the law of the EU Member State where the data exporter is domiciled. If such law does not allow the exercise of rights belonging to the authorised third party, they are governed by the law of another EU Member State that allows the exercise of those rights. The Parties agree to be governed by the law of the *personal data exporter*..]

**MODULE 4: Transfer from Processor to Controller**

These clauses are governed by the law the country that such law allows the exercise of rights belonging to the authorised third party. The Parties agree to be governed by the law of the *personal data exporter.]*

***Clause 18***

**Choice of court and jurisdiction**

**MODULE 1: Transfer from Controller to Controller**

**MODULE 2: Transfer from Controller to Processor**

**MODULE 3: Transfer from Processor to Processor**

Any disputes arising from these clauses will be settled by the courts of the EU Member State.

The Parties have agreed to be governed by the *personal data exporter's* courts.

The data subject may also bring legal proceedings against the data exporter and/or the data importer before the courts of the Member State where the data subject is usually resident.

The Parties agree to submit to the jurisdiction of these courts.

**MODULE 4: Transfer from Processor to Controller**

Any disputes arising from these clauses shall be settled by the courts of the *personal data exporter.*

Where these standard contractual clauses refer to any annexes, their wording is deemed to be determined by Commission Implementing Decision (EU) 2021/914.

In Prague dated 19 July 2023