Generally Binding Conditions for Processing Personal Data by the Processor and Other Persons

CONTENTS

I. Introductory Statement

In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Regulation on the Protection of Personal Data) (*hereinafter the "**GDPR**"*), the following Generally Binding Conditions for Processing Personal Data by the Company and Other Persons (*hereinafter the "**Processing Conditions**"*) shall enter into force as of 25 May 2018.

These Processing Conditions were accepted together with other documents governing the rights and obligations relating to personal data protection at **Smartwings, a.s.., CRN: 25663135, with its registered office at Prague 6, K Letišti 1068/30, 160 08** (hereinafter "***SW CZ***"). SW CZ is the parent company of other joint administrators, namely **Smartwings Slovakia, s.r.o.**, with its registered office at Ivanská cesta 30/B, Bratislava 821 04 (hereinafter "*SW SK*"), **Smartwings Hungary Kft.**, with its registered office at Wesselényi u. 16/A, Budapest, 1077, Hungary *(hereinafter "**SW HU**")*, **Smartwings Poland Sp. z o.o.**, with its registered office at ul. Gordona Bennetta 2B, Warszawa, 02-159, Poland *(hereinafter "**SW PL**")* and **Smartwings Germany Gmbh**, with its registered office at Theatinerstraße 23, 80333 München, Germany *(hereinafter "**SW DE**")* (*hereinafter jointly referred to as "**SW**" or the "**Controller**"*). These Terms and Conditions separately govern the relationship of each of the controllers with the processor, that being according to the circumstances of the primary contract, unless a written processing agreement is concluded between the parties, which deviates from the provisions of these Terms and Conditions.

The Controller will conclude a written Processing Agreement on Personal Data Processing (*hereinafter the "**Processing Agreement**"*) with each Processor, which will bindingly refer to these Processing Conditions. If a written Processing Agreement is not concluded with the Processor, the relationship established by the Primary Contract shall always be governed by these Processing Conditions and these terms shall become part of the Primary Contract.

These Processing Conditions bindingly govern the rights and obligations of the Controller and the Processor when the Processor processes the personal data of data subjects for the Controller in connection with the Service that the Processor carries out for the Controller or with the Products that the Processor provides for the Controller. Processors are required to familiarize themselves with these Processing Conditions and process Personal Data in accordance with them. In addition to the Processor's undertaking to process Personal Data in accordance with these

Processing Conditions, the Personal Data will be specified in the Processing Agreement in accordance with the first sentence of Article 28 (3) of the GDPR. In the event of a need arising from providing a particular Service or Product, the obligations and rights of the parties to the Processing Agreement may be governed differently from these Processing Conditions; in such a case the different arrangement in the Processing Agreement has priority.

A specimen of the Processing Agreement forms part of these Processing Conditions as **Appendix 1**.

Unless otherwise specified in the Processing Agreement, the contact person responsible for the personal data protection agenda for the purpose of the Processor processing Personal Data, i.e. the person designated for communication and cooperation between the Controller and the Processor for each of the joint Controllers separately, namely at the headquarters of the specific Controller published in the public register. The Joint Controllers have also designated as a joint contact point: **Smartwings, a.s., CRN: 25663135, with its registered office at Prague 6, K Letišti 1068/30, 160 08, Czech Republic and the email link law@smartwings.com**.

The representative for SW CZ is:

KUBEČKA & PROKOP, advokátní kancelář s.r.o., with its main office at Kladská 1489/5, Vinohrady, 120 00 Praha 2, Czech Republic, email: dpo@smartwings.com.

II. Definition of terms

1. For the purposes of the Processing Conditions and other documents associated with data protection, the Controller shall use terms that are understood as:
    - **"Controller"** the company Smartwings, a.s., CRN: 25663135, with its main office at Praha 6, K Letišti 1068/30, postcode 16008, Czech Republic or Smartwings Slovakia, s.r.o., with its main office at Ivanská cesta 30/B, Bratislava 821 04, Slovak Republic, Smartwings Hungary Kft., with its main office at Wesselényi u. 16/A, Budapest, 1077, Hungary, Smartwings Poland Sp. z o.o., with its main office at ul. Gordona Bennetta 2B, Warszawa, 02-159, Poland, or Smartwings Germany Gmbh, with its main office at Theatinerstraße 23, 80333 München, Germany, that being always according to the circumstances of the primary contract;

- "**Personal data**" **is** any information about an identified or identifiable natural person (hereinafter also referred to as the "data subject") forwarded by the Controller to the Processor or by a provably designated entity and processed by the Processor for the Controller and/or in connection with the Primary Contract;
- "**Processor**" any entity processing Personal Data for the Controller and on behalf of the Controller;
- "**Sub-processor**" any other Personal Data processor (including any third party) engaged by the Processor to process Personal Data on behalf of the Controller. The Processor and Sub-processor is entitled to engage another Sub-processor to process Personal Data under the terms and conditions set forth in these Processing Conditions;
- "**Approved Sub-processor"** (a) the Sub-processor listed in Appendix 3 to the Agreement on Processing Personal Data (transferring Personal Data pre-authorized by the Administrator); and (b) other partial Sub-processors Pre-authorized in writing by the Administrator in accordance with Article IX of these Processing Conditions;
- "**Primary Contract"** a valid and effective legal transaction entered into between the Controller and the Processor, under which the Processor carries out a particular Service for the Controller or provides certain Products (specifically defined in the Processing Agreement;
- "**Instruction**" any instruction the Controller gives to the Processor concerning Personal Data processing. The Processor must prove the existence and content of the Order at any time whilst processing Personal Data;

- "**Breach of personal data security" a** personal data breach that leads or may directly lead to the accidental, unauthorized or unlawful destruction, loss, alteration or unauthorized provision or disclosure of Personal Data that is transmitted, stored or otherwise;
- "**Regulations on Personal Data protection**" the GDPR and all legislation governing personal data at the national level and in the European Economic Area or the EU that apply to the Controller or Processor;
- "**Standard contractual clauses"** means standard contractual clauses for transferring personal data to processors established in third countries that have been 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"** any country outside the EU or the European Economic Area, except for cases where this country is the subject of a valid and effective European Commission decision on adequate personal data protection in third countries;
- "**Erasure**" irreversibly removing or destroying Personal Data so that it cannot be restored or reconstructed;
- "**Principles for processing personal data**" are the principles of legality, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality in the sense of the GDPR.

2. **Any other general terms not stated or undefined in these Processing Conditions, Processing Agreement, Primary Contract or other documents adopted by the Controller in relation to personal data protection shall be interpreted in accordance with the GDPR**

III. General Conditions for the Processor processing Personal Data

1. **In the course of performing the Primary Contract for the Controller the Processor is entitled to process Personal Data on behalf of the Controller in accordance with and under the terms and conditions set forth in these Processing Conditions, unless the Processing Agreement specifies otherwise, the Controller's Instructions and the Personal Data Protection Regulations**
2. **The processor is entitled to process Personal Data solely for the purpose of fulfilling the Primary Contract or for a performance provided on the basis of the Primary Contract**. The purpose of processing and other processing conditions are determined by the Controller and, if the Processor violates this rule, it is considered to be the person of the controller in relation to such processing. The specific purpose of the processing and other specifications for processing are regulated in the Processing Agreement
3. The Processor undertakes to comply with all the technical and organizational measures ensuring the requirements of these Processing Conditions, the Personal Data Protection Regulations and the Processing Agreements are met. The technical and organizational measures, for the purposes of processing Personal Data, are defined in Appendix 2 to these Processing Conditions with the possibility of further specifications in the Processing Agreement.

4. The Processor is required to obtain, renew and retain all the necessary licenses, authorizations and permissions needed for processing Personal Data as required by the applicable and effective Personal Data Protection Regulations.

5. The Processor is obliged to inform the Administrator without delay, but no later than within 3 days of delivery of the Instruction, that, in his/her opinion, the Instruction is not in accordance with the Personal Data Protection Regulations, the Processing Agreement, these Processing Conditions or violates them in another manner.

IV. Transferring Personal Data and processing in a third country

1. The processor is not authorized to process/facilitate processing, especially transfer, distribute, modify, disclose, change, publish or allow the publication of, or otherwise disclose Personal Data to another third party other than in accordance with these Processing Conditions, the Processing Agreement or with the Instruction except for the transmission of Personal Data as required by EU or a Member State's law (*hereinafter also a referred to as a "**legal transfer requirement**"*) to which the Processor is subject. The Processor is obliged to inform the Controller about a legal transfer requirement for Personal Data sufficiently in advance before starting the transfer, unless the relevant legislation prohibits informing about the transfer of Personal Data.

2. The Processor is obliged to restrict the extent of the Personal Data transferred to a minimum, unless the applicable legislation regulates the extent of the personal data transferred.

3. The Processor is not entitled to process Personal Data in a third country without the prior written consent of the Controller, not even by means of a Sub-processor, unless further specified or otherwise specified in the Processing Agreement

4. Without further authorization Processors shall transfer Personal Data for processing to recipients in third countries and to the international organization listed in Appendix 3 to these Processing Conditions (*hereinafter the "**transferral of personal data approved by the Controller**"*), provided such a person meets the requirements set out in Article IX of these Processing Conditions. The Processor is obliged to inform the Controller about the transferral of personal data approved by the Administrator to the persons listed in Appendix 3, without delay, but no later than within 3 days

5. At the request of the Controller, the Processor shall immediately enter into an agreement with the Controller, including Standard Contract Clauses or similar clauses that may be required by the Personal Data Protection Regulations if it concerns any processing of Personal Data in a third country whatsoever. The Processor is obliged to ensure that the legal transaction under the previous sentence is concluded with the Controller and any other Sub-processor.

V. Persons authorized to process Personal Data at the Processor

1. The Processor is required to adopt all necessary measures to verify employees or other persons who process Personal Data at the Processor. The Processor is obliged to ensure only verified and reliable employees or other persons (also referred to as "Authorized Persons") have access to Personal Data and only to the extent necessary to fulfil the Primary Contract. The Processor regularly verifies the Authorized Persons and reviews their reliability

2. The Processor keeps a list of Authorized Persons with access to Personal Data and regularly updates it so it corresponds to the facts.

3. The Processor is obliged to inform Authorized Persons about the fact that Personal Data are data subject to protection under the Personal Data Protection Regulations, their processing is governed by the Personal Data Protection Regulations, as well as the obligations set forth by the Processing Conditions, the Processing Agreement and the Instructions. The Processor is required to explain the obligations under the previous sentence to the Authorized Persons in a clear and unambiguous manner and to get an undertaking from them that they will adhere to the obligations.

4. The Processor is obliged to maintain confidentiality about the Personal Data and its processing at the Controller and the Processor. The Processor is required to contractually bind the Authorized Persons to confidentially for the duration of the employment or other legal relation between the Processor and the Authorized Person, which also includes a reasonable time after termination of such relationship, that being in the event that a legal or professional duty of confidentiality does not relate to them, where in such a case the Processor is obliged to inform the Authorized Person of the legal/professional duty of confidentiality.

5. The Processor is obliged to provide regular and adequate training and certification for the Authorized Persons in connection with the Personal Data Protection Regulations or the Instructions.

6. The Processor is required to ensure that when processing Personal Data the Authorized Persons:

   - only use safe hardware and software and adhere to the principles of safe use of computer technology;
   - are subject to and observe the processes of user authentication and logging in when accessing Personal Data;
   - prevent unauthorized reading, destruction, deletion or other loss, alteration or unavailability of Personal Data, do not make copies of Personal Data carriers for purposes other than work and prevent such behaviour by other persons, including any disclosure or provision to an unauthorized person;
   - immediately, but no later than within 24 hours of an occurrence, report any reasonable suspicion of a threat to the security of the Personal Data, that being to the person referred to in Article 1 of these Processing Conditions.

VI. The Processor's cooperation when fulfilling the Controller's duties

1. The processor is obliged to cooperate with the Administrator when fulfilling the Controller's duties with regards to the data subjects, including a response to requests to exercise the data subjects' rights pursuant to the Personal Data Protection Regulations and by means of appropriate technical and organizational measures, an furthermore when fulfilling the Controller's other duties pursuant to the Personal Data Protection Regulations.

2. The Processor is obliged to cooperate within a reasonable time period if these Processing Conditions, the Processing Agreement or the Controller's Instruction do not determine a specific deadline.

3. For the purposes of these Processing Conditions, cooperation is understood to be assistance in ensuring compliance with the obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to the Processor and only in relation to processing Personal Data

4. Cooperation primarily involves:
    - providing and making available all information, data and documents relating to Personal Data or necessary to demonstrate compliance with the applicable and effective Personal Data Protection Regulations, these Processing Conditions, the Processing Agreement and the Instructions;
    - assistance and consultation on the part of the Processor which is commensurate and reasonable with regards to the specific obligation that relates to the Controller;
    - implementing additional technical and organizational measures that the Controller can reasonably require beyond the legal and contractual obligations so that he can effectively respond to complaints, notifications or requests;
    - assistance in all cases of a data protection impact assessment that are required by Article 35 of the GDPR and with any prior consultations with any of the controller's supervisory authorities, as required by Article 36 of the GDPR
5. The Processor is required, without undue delay, but no later than within 7 days of receiving a request, to make it known that it received a request concerning Personal Data from a data subject, a supervisory authority or any other entity pursuant to the Personal Data Protection Regulations.
6. The processor is obliged to allow audits and inspections by the Controller or another auditor authorized by the Controller (*hereinafter also referred to as the "**authorized auditor**"*) in all places where Personal Data is processed. The Processor is obliged to cooperate and allow the Controller/authorized auditor to check, audit and copy all records, processes and systems so that the Controller can verify that the Personal Data is processed in accordance with the applicable and effective Personal Data Protection Regulations, these Processing Conditions, Processing Agreement and the Instructions
7. The processor is obliged to provide and hand over to the Controller any documents concerning the processing of Personal Data and fulfilling the duties of a Processor
8. The Processor is required to immediately notify the Controller if, in his/her opinion, the right to an audit under this article is at variance with the Personal Data Protection Regulations.
9. The Processor is also required to ensure the Controller's rights, pursuant to this Article, are also exercised at all its Sub-processors.

VII. Personal Data Security

1. In accordance with Article 32 (1) of the GDPR, i.e. taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
2. The Processor is required, to a reasonable extent, to ensure at least the following when processing Personal Data:
   - the pseudonymization and encryption of personal data;
   - the ability to ensure 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;
   - a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of Personal Data processing;

   where the specific conditions for Personal Data security are contained in Appendix 2 to these Processing Conditions and may also be specified in the Instructions or the Processing Agreement.
3. If the parties to the Primary Contract have not entered into a written Processing Agreement or an appendix to the Primary Contract or a Processing Agreement that extends these technical and organizational measures, then Article 7 of these Conditions is the minimum extent of the measures that the personal data processor must accept
4. When assessing a suitable level of security, the Processor shall take into account the risks involved in processing Personal Data, in particular the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized access to transmitted, stored or otherwise processed Personal Data.
5. In the case of the processing personal data for multiple controllers, the Processor is obliged to process the Controller's Personal Data separately in order to avoid mixing and joint processing.

VIII. Personal Data Security Breaches

1. In the event of a personal data security breach, the Processor is obliged to inform the Controller immediately, but no later than within 24 hours, that there was a personal data security breach or there is a reasonable suspicion of a personal data security breach (*hereinafter also referred to as a "**security breach notification**"*).
2. The Processor is required to provide the Controller with sufficient information to enable him to fulfil all his obligations concerning the reporting and notifying about personal data breaches pursuant to the Personal Data Protection Regulations. Notification of a security breach must at least contain:
    - a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the specifications and approximate number of personal data records concerned;
    - the name and contact details of the Processor's data protection officer or other contact point where more information can be obtained;
    - a description of the likely consequences of the personal data breach and the risk;
    - a description of the measures taken or proposed to be taken to address the personal data breach;
    - a description of the measures taken or proposed to mitigate the possible adverse effects of address the personal data breach.
3. The Processor is required to cooperate with the Controller, to provide all possible cooperation to investigate, mitigate, remove and remedy the Personal Data breach and implement the Controller's Instructions imposed for this purpose.
4. Pursuant to the Personal Data Protection Regulations, the Controller is entity responsible for informing about Personal Data security breaches. The Processor has no authorization to notify any person about a Personal Data security breach without the prior, demonstrable consent of the Controller if this this obligation is not imposed by EU law or the law of the Member State that relates to the Processor. The Processor is obliged to immediately inform the Controller about the legal requirement to inform about the Personal Data security breach prior to announcement of the notification. The Processor is obliged to provide the Controller with the text of the notification for comments, that being in advance and in good time, before the expiration of any deadlines relating to the Processor for the purpose of informing about the breach of security. The Processor is obliged to modify the

notification according to the Controller's Instructions if it complies with the EU and Member State laws that relate to the Provider and correspond to the security breach. The Processor is obliged to consider any other possible comments by the Controller for the notification.

IX. Sub-processors

1. On the basis of these Conditions, the Controller grants the Processor a general permission to engage another processor in processing on the basis of a primary contract, except when:
   a) no written Processing Agreement has been entered into between the Controller and the Processor which includes these conditions;
   b) a written agreement between the Controller and the Processor excludes processing by another processor or determines otherwise;
   c) processing is carried out by sub-processors in third countries and there is no Commission decision on the appropriate level of personal data protection or any other bilateral or multilateral international treaty guaranteeing this appropriate level of personal data protection.
   d) The Administrator has taken back his consent, that being even after starting on the processing, because he considers that the Sub-processor involved does not meet these Conditions.
2. The Processor may engage another Sub-processor to process the Personal Data even if he or she cannot be engaged in the processing pursuant to the preceding paragraph of this Article, provided that such persons are listed in the document a specimen of which is set out in Appendix 3 to these Processing Conditions (Approved Sub-processor). The Processor is obliged to inform the Controller about engaging an Approved Sub-processor listed in Annex No. 3, without delay, but no later than within 3 days prior to the intended engagement. The Controller is entitled to withdraw his consent to the involvement of another processor at any time and at the same time may unilaterally exclude the Approved Sub-processor from further processing, because he believes that the Sub-processor involved does not meet these Conditions.
3. When a Sub-processor is engaged the Processor must:

- inform the Controller of all the processing activities that the Sub-processor will carry out for the Processor;
- ensure that when the Sub-processor processes Personal Data it is governed by and in accordance with these Processing Conditions, the Processing Agreement, the Instructions and the Personal Data Protection Regulations in order to ensure an appropriate level of Personal Data protection. In order to fulfil the obligation under the previous sentence, the Sub-processor shall enter into a written agreement with the Processor (*hereinafter the "**Sub-processor Agreement**"*) which will determine the Sub-processor's obligations and conditions in accordance with these Processing Conditions, the Processing Agreement, the Instructions and the Personal Data Protection Regulations, including a definition of specific technical and organizational measures;
- ensure an appropriate level of protection for the Controller's Personal Data, including adequate safeguards for implementing suitable technical and organizational measures pursuant to this Processing Agreement, the Primary Contract, the Instructions and the applicable and effective Personal Data Protection Regulations;
- verify and periodically check that the Sub-processor processes Personal Data in accordance with the Sub-processing Agreement and not in violation of these Processing Conditions, the Processing Agreement, the Instructions and the Personal Data Protection Regulations. The Processor informs the Controller in writing about the results of the inspection within 2 weeks of having carried it out;
- in the event of transferring Personal Data outside of the European Economic Area, the Controller is required to ensure that Standard Contractual Clauses or other mechanisms are in the contracts between the Processor and the Sub-processor and that they have been previously approved by the Controller to ensure adequate protection of the transferred Personal Data.

4. If the Sub-processor violates their obligations, the Processor is responsible to the Controller for meeting the Sub-processor's obligations
5. After the prior written consent of the Controller, so-called processor chains are possible, i.e. the conclusion of a contract for processing personal data between Sub- processors is possible. The contracts entered into between Sub-processors must comply with the terms and conditions of these Processing Conditions, the Processing Agreement, the Instructions,

and Personal Data Protection Regulations in order to ensure an appropriate level of Personal Data protection. It is not possible to have processor chains without the Controller's prior written consent.

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

X. Ending Personal Data Processing

1. After termination of the Primary Contract or ending Personal Data processing for any other reason on the basis of a written Instruction, the Processor, within a reasonable time and in any event not later than 45 calendar days, must either:

   a) return a complete copy of all Personal Data to the Controller by securely transferring the data files in the format specified in the Controller's Instruction and likewise safely and demonstrably delete all other copies of the Personal Data processed by the Processor or any other Sub-processor, or

   b) safely and demonstrably delete all copies of Personal Data processed by the Processor or by any other Sub-processor.

2. The Processor must provide the Controller, without undue delay, but no later than within 7 days, a written certificate of having met the obligations pursuant to this Article.

3. Without prejudice to the obligation under paragraph 1 of this Article, the Processor shall continue to be authorized to process Personal Data to the extent required by EU or Member State legislation relating to the Processor. Processing under the preceding sentence may only take place for a period of time, for the purpose of and in accordance with the law, where the Processor is obliged to primarily ensure the Personal Data have adequate protection and confidentiality.

XI. Codes of Conduct and Certification

1. The Processor shall, at the request of the Administrator, adhere to the relevant Code of Conduct approved under Article 40 of the GDPR. Until the Code of Conduct has been approved by the Authority pursuant to the previous sentence, the Processor will follow the Code published on the Controller's web site.

2. At the request of the Controller, the Processor is required to obtain the relevant certificate pursuant to Article 42 of the GDPR

3. The Processor is obliged to ensure compliance with the Code of Conduct or its relevant parts without undue delay and to ensure that the Sub-processors acquire the certification.

XII. Standard Contractual Clause

1. If a Processor is resident in a third country, the relationship between the Processor and the Controller shall be governed by the Standard Contractual Clause, as amended by the Annex to the Commission Decision of 5 February 2010 (notified under document number C (2010) 593), that being in the sense of Article 26 (2) of Directive 95/46/EC and Article 45 (9) of the GDPR where the Contracting Parties declare that, if the Commission amends, replaces or repeals its Decision by a decision taken pursuant to paragraph 3 or 5 of Article 45 of the GDPR, the contractual relationship will be governed by the new Commission Decision.

2. The preceding paragraph shall not apply if the Commission has decided that this third country, a certain territory or one or more specific sectors in this third country provide an adequate level of protection or where there is an international treaty binding on both Contracting Parties on the basis of which an adequate level of protection is ensured.

3. The full wording of the standard contractual clause is contained in Appendix 4 to these Conditions.

Appendix 1 Processing Agreement

Agreement on Processing Personal Data

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

Smartwings, a.s., CRN: 25663135

With its registered office at Praha 6, K Letišti 1068/30, 160 08

(hereinafter also "SW CZ" or the "Controller")

and

……*, CRN: ……*

with its registered office at: ……*

represented by: ……*

acting: ……*

(hereinafter the "Processor")

(The Controller and the Processor collectively also referred to as the "Contracting Parties")

Article I. – Introductory Statement

1. The Contracting Parties declare that the Processor carries out the Service/provides the Products for the Controller on the basis of Contract ..... * dated ..... * *(hereinafter the "**Primary Contract**")* and, in connection with the Primary Contract and on behalf of the Controller, processes the Personal Data of data subjects transferred by the Controller or by a demonstrably designated entity
2. The Contracting Parties have agreed that the personal data processing will be governed by the Generally Binding Conditions for Processing Personal Data by the Processor and Other

Persons (hereinafter the "Processing Conditions") published on the Controller's web site, that being in accordance with the current version of the Processing Conditions.

3. The Processing Conditions become a binding and indispensable part of this Processing Agreement

4. The Processor declares that he/she has become acquainted with the Processing Conditions and is required to abide by them when processing personal data

Article II – Specification of the Personal Data and their Processing

1. Kind and type of personal data:

   ☐ Personal data:……

   ☐ Special categories of personal data pursuant to Article 9 of the GDPR:……

2. Duration of processing personal data: for the duration of the Primary Contract. Termination of the Primary Contract does not affect the Processor's rights and obligations, which by their nature or according to this Agreement or the Processing Agreement should continue after the termination of the Primary Contract

3. Nature of processing:

   ☐ Processing

   ☐ Automatic processing

   ☐ Profiling or automatic decision making

4. Purpose of processing:……

5. Category of the data subjects:…….

Article III - Final Arrangements

1. The terms used in this Agreement shall be interpreted in the sense of the Processing Conditions.

2. This Agreement shall enter into force and effect with the signature of both Contracting Parties.

3. This Agreement may be only amended by written addenda numbered in ascending order and signed by both Contracting Parties. This provision is without prejudice to the possibility of changing the Processing Conditions and the Controller assigning Instructions for processing the Controller's Personal Data.
4. If any provision of this Agreement is found to be invalid or become invalid, this shall be without prejudice to the other provisions of this Agreement. The Contracting Parties to this Agreement undertake to conclude an amendment without delay in order to negotiate the new, valid provisions, instead of the invalid provisions, which are closest to the purpose of the invalid provisions.
5. This Agreement is drawn up in 2 copies with the validity of an original, each Contracting Party receiving one copy each.

In……..dated…… In……..dated……

……. …….

Controller Processor

Appendix 2 – Technical and Organizational Measures

1. General Provisions

The Processor is obliged to adopt binding documentation governing the technical and security measures for the protection and security of the processed Personal Data (hereinafter the "Security Documentation").

The Processor is obliged to familiarize its personnel with the Security Documentation and these Processing Conditions and to carry out 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.

All passwords used must meet the requirements for a very strong password, including length, character complexity and unrepeatability.

2. Responsible Persons and Authorized Persons

The Processor is required to identify the specific persons responsible for ensuring and implementing technical and organizational measures, resolving suspicions and breaches of Personal Data security and the contact person for the Controller and the data subject. The Processor is obliged to clearly define the role and responsibilities of the persons pursuant to the previous sentence.

The Processor keeps a list of all the devices on which Personal Data is processed. This list is regularly updated.

Authorized persons processing Personal Data pursuant to Article V of these Processing Conditions have clearly defined tasks and activities when processing Personal Data and process personal data only to the extent necessary to meet the Processor's obligations under the Primary Contract, the Processing Agreement and these Processing Conditions.

Upon ending the cooperation with the Authorized Person (e.g. terminating the main employment relationship, etc.), the Processor is obliged to ensure that these persons are denied any access to the Personal Data.

3. Entry to the Processor's Premises

Entry to the premises where personal data is processed (also referred to as the "processor's premises") must be protected, at least by a security key lock or an intruder alarm system. It is forbidden to provide unauthorized persons with access to keys and codes for the alarm. At the very least the following duties must be respected when handling keys, alarm codes and access to the Processor's premises:

- it is forbidden to lend or entrust the key to other persons or transfer it to others as a deposit. It is forbidden to make a copy of the key without the consent of the employee designated as being responsible for security at the Processor's premises (*also referred to as the "security officer"*)
- the access code is protected by confidentiality and must not be imparted to any other person. It is forbidden to record the alarm code in any form, except recording it for the needs of the security officer;
- when entering the Processor's premises, it is a duty to ensure that doors with controlled access are closed and that unauthorized persons cannot enter the Processor's secured areas;
- it is essential to protect both the key and the access code against loss, theft, misuse, destruction or damage.

It is necessary to observe at least the following principles during a visit to the Processor's premises;

- the visitor cannot be left without supervision anywhere where the Controller's Personal Data is being processed;
- an unknown person at the Processor's premises who is unaccompanied must be identified and taken to the staff member they would like to visit or handed over to the responsible person.

Allowing access to data centres, server rooms and other relevant technical rooms (*also referred to as "technical rooms"*) is subject to the approval of the Processor's Responsible Person. Visitors to the technical rooms must always be accompanied by the Processor's Responsible Person.

4. Computers and Laptops

When handling computers and laptops, the following minimum requirements must be upheld:

- the assistance of a responsible IT worker is essential for connecting, disconnecting and any other manipulation;
- the hard drive must be encrypted and secured with a password. After turning on the computer and laptop system a password must be requested. It is forbidden to save and automatically enter the password. The password must be changed at regular intervals
- Personal Data may only be stored on the Processor's password-protected and encrypted servers and can only be processed on encrypted and password-protected network drives and in the framework of relevant legal applications;
- it is forbidden to share local disks, CD-ROMs, and so on;
- a computer and laptop cannot be left unattended when switched on. If it is necessary to leave for a while without switching off, the computer or laptop must be secured by a password
- wireless technology must be turned off by default. It can only be turned on if it is necessary to connect to a specific network;
- the Processor can only use legally acquired software, which is installed by the responsible IT worker in accordance with the pertinent rules and procedures;
- it is forbidden to install and distribute illegally acquired software and text / audio / video content or to store it on the computer or laptop;
- the computer and laptop must be protected by a firewall, antivirus, and other security settings that only the responsible IT worker is allowed to activate, update and deactivate where updates and tests are regularly run. In the event of the suspected presence of a virus or other threat, the Processor's employee is obliged to immediately inform the responsible IT worker;
- the Processor's employees have separate user accounts except in such a case when it is necessary for persons using the same user account to have the same duties, tasks and responsibilities when processing Personal Data.

5. Protecting Portable Devices

Portable devices are considered to be laptops, mobile phones, PDAs, tablets, etc.. The following minimum requirements must be met when handling portable devices:

- the portable device must be protected from access by unauthorized persons and must not be left unattended by the Processor's employee except when this is not objectively possible;
- when carried, the portable device must be located within immediate reach and under the control of the Processor's employee, except when this is not objectively possible;
- in the event of loss or theft of a portable device, the Processor's employee must immediately inform the person responsible and the superior. Depending on the technical options available, the Processor is required to attempt to block or erase the portable device with the help of the responsible IT personnel;
- the portable device must be protected by a password, if it is objectively possible, and this password must be required whenever the portable device is used;
- the Processor's employees may not use their own portable device for processing Personal Data without the prior consent of the Processor where this consent may only be given in an exceptional situation;
- Personal Data stored on portable devices can only be stored on a password-secured and encrypted repository. Otherwise, it is not possible to use the portable device to store Personal Data;
- it is forbidden to connect a portable device to another device that is not under the Processor's control (e.g. computers in Internet cafes, print shops, private computers, etc.).

In cases where it is not objectively possible to protect a portable device from access by unauthorized persons, when it is not possible to be in immediate reach and under the control of the Processor's employee and in other cases where there is the threat of Personal Data security breaches, the portable device must be protected by a security cable or another mechanically safe manner and furthermore protected at least by a password or other possible means of protection, that being to the widest extent possible, so as to ensure an appropriate level of security.

In order to exchange Personal Data between the Processor's employees, it is essential to use a shared repository within the Processor's network and not to use portable media except for an

exceptional and justified case using a password and encryption, where it is necessary to permanently delete the Personal Data from the portable media without undue delay after it has been exchanged.

6. Using the Internet, Email and Remote Access to the Processor's Network

The following minimum requirements must be met when using email and the Internet:

- it is only possible to access the Internet through the Processor's IT infrastructure;
- it is forbidden to upload and save Personal Data on public storage servers;
- communication by means of the Internet is encrypted using cryptographic protocols;
- only work emails, which may not be used for private purposes, can be used when processing Personal Data;
- Personal Data transmitted by email must be password protected and encrypted, otherwise it cannot be transmitted;
- the use of automatic forwarding for e-mail messages to e-mail addresses outside the company network is not allowed;
- in the event of email communications with more than one person, where at least one person is a person working externally to the Processor, it is necessary to use the Bcc feature;
- when using remote access to the Processor's local network only the Processor's workstations or laptops and a VPN connection managed by the Processor are allowed to be used. It is forbidden to create remote connections from other workstations that are not under the Processor's control;
- in order to use remote access, upon prior approval by the responsible person, the Processor's employee must have a certificate assigned and installed. To log in to the VPN, the Processor's employee must identify the following data: login, password, certificate and domain name.

7. Data Backup and Deleting Personal Data

The Processor is required to continuously back up Personal Data in a timely manner so they are not destroyed, damaged, etc.

When removing any portable device, it will first be overwritten to erase the Personal Data. If it is not possible to overwrite it, it will be disposed of physically.

Any documents containing Personal Data that are to be disposed of must be shredded.

Documentation must be kept about overwriting, shredding, and disposal of devices.

Appendix 3 List of Sub-processors and Transferral to Recipients in Third Countries

I. Transferral of personal data approved by the controller pursuant to Article IV (4) of the Processing Conditions

No.	Approval of recipient	Main office	Processing specifications
1.			
2.			

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

No.	Approved Sub-processor	Main office	Processing specifications
1.			
2.			

Appendix 4 Standard Contractual Clause

An exporter of personal data, who is a personal data controller pursuant to these Processing Conditions and Primary Contract and the Personal Data Importer, who is the processor of the personal data pursuant to these Processing Conditions and the Primary Contract together, in order to meet the conditions of Article XII of these Processing Conditions (individually the "Party" together the "Parties") as part of the Personal Data Processing Agreement, also enter into a contractual clause with the following wording:

Clause 1

Definitions

For the purposes of the clauses:

(a) "personal data", "special categories of data", "to process/processing", "controller", "processor", "data subject" and "supervisory authority" have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) "data exporter" is understood to be the controller who transfers personal data;

(c) "data importer" is understood to be a processor who undertakes to receive personal data from the data exporter to be processed on behalf of the data exporter after transferral in accordance with his instructions and the terms of those clauses and who is not subject to a third country system ensuring adequate protection within the meaning of Article 25 (1) of Directive 95/46/EC;

(d) "sub-processor" is understood to be a processor hired by the data importer, or another of the data importer's sub-processors, who undertakes to receive personal data from the data importer, or another of the data importer's sub-processors, that is exclusively intended for processing activities on behalf of the data exporter after being transferred in accordance with the data exporter's instructions, the conditions set out in the appendix and the terms of the written contract on sub-processing;

(e) "the applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) “technical and organizational security measures” means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and, in particular, the possible special categories of personal data are given in the contract for processing personal data (replacing Appendix 1), which forms an integral part of the clauses.

Clause 3

Third party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

(1) The data importer agrees and warrants::

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about: | (i) | any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation; | (ii) | any accidental or unauthorized access; and | (iii) | any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any

successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. | The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

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

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same

conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

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

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Clause 13

Appendices specified by the Annex to Commission Decision of 5 February 2010 (notified under document number C (2010) 593) within the meaning of Article 26 (2) of Directive 95/46/EC and Article 45 (9) of the GDPR

Appendix 1 and Appendix 2 are replaced by the provisions of the Personal Data Processing Agreement and the Primary Contract, where this contract documentation describes the activity of the Data Exporter, the Data Importer, the Data Subjects, data categories, special data categories, the processing process and the undertaking of the data importer to adopt the organizational and technical measures specified in the Conditions.

Prague, 3.27.2019