

**Standard contractual clauses regarding transfer of personal data from the Community to third party countries (transfer between controllers), hereinafter referred to as „clauses” applicable to contracts made between ROHLIG SUUS and a Carrier**

## Definitions

Under these Clauses:

- a) „personal data”, „special data categories/ sensitive data”, „to process/ processing”, „data controller”, „data processing entity”, „data subject”, and „supervisory authority” shall have the same meaning as in the Regulation 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data repealing Directive 95/46/WE (General Data Protection Regulation) <sup>1</sup>, hereinafter referred to as GDPR, where „supervisory authority” shall refer to the appropriate supervisory authority on the territory of the country where the transferor’s seat is located);
- b) „data transferor” shall refer to the data controller who is transferring personal data; insofar as this Contract applies, this shall be ROHLIG SUUS;
- c) „data receiver” shall refer to the data controller who agrees to receive personal data from the transferor for further processing on the terms and conditions laid out in these clauses, who is not subject to third party country data safeguards; insofar as this Contract applies, this shall be the Carrier;
- d) „clauses” shall refer to the contractual clauses herein which constitute separate documents and do not include trade terms as agreed on between the parties in a separate sales agreement.

The details of data transfer (including the types of personal data) are provided in Attachment B which forms an inseparable part of these clauses.

## I. Data Transferor’s Duties

The data transferor agrees to the following conditions and warrants as follows:

- a) that it will collect, process and transfer data in line with applicable laws;
- b) that it has taken legitimate steps to establish whether the data receiver will be able to meet its legal obligations as laid out in the herein clauses;
- c) that on receiver’s demand, it will make available copies of applicable data protection regulations of the country in which the transferor is headquartered and will notify the receiver where to look for information on such regulations (where appropriate; this shall not include legal advice);
- d) that it will provide exhaustive and timely responses to queries from the supervisory authority and the data subject regarding processing by the data receiver, unless the parties have agreed that such responses will be provided by the data receiver in which case the transferor

<sup>1</sup> Official Journal of the EU L/119, p. 1

will continue to provide responses in legitimate circumstances and to a legitimate extent if the receiver cannot or doesn't wish to provide such responses. Responses shall be provided within a reasonable timeframe;

- e) that on demand from the data subject, or beneficiaries – a third party as defined in point 3 of these clauses, it shall make available a copy of the herein clauses provided they do not contain confidential information in which case the transferor may remove such data prior to making them available. In the event when such data is removed, the transferor shall inform the data subject in writing of the reason for the removal and of the subject's right to notify the supervisory authority of such removal. The transferor shall adhere to a decision by the supervisory authority regarding full access of data subjects to the clauses, provided the subjects undertake to keep confidential information that has been removed. At the request of the supervisory authority, the transferor shall make available a copy of the herein clauses. The data receiver shall take over responsibility for ensuring compliance with the provisions of this point.

## II. Data Receiver's Duties

The data receiver agrees to the following conditions and warrants as follows:

- a) that it will apply appropriate technologies and administrative measures to safeguard personal data against accidental or unlawful damage, accidental loss, modification, disclosure or provision to unauthorized individuals, and that it will ensure a level of protection appropriate for the level of risk that exists when data are processed and for the nature of those data;
- b) that it will apply procedures to safeguard the safety and confidentiality of personal data by third parties who also process data which it has authorized to process such data. All individuals acting on authority from the data receiver, including those processing data, undertake to process personal data only on instruction from the data receiver. This provision shall not apply to individuals with authorized access to personal data or having such authority granted to them by law;
- c) that there is no reason to believe that the legal regulations it is subject to could have substantial negative implications for the guarantees set out in these terms and conditions, and in the event that such shall occur, it will notify the data transferor of this (who will notify the supervisory authority if necessary);
- d) that it will process personal data for the purposes outlined in Attachment B and that it falls under the jurisdiction of the supervisory authority which warrants adherence to the obligations as laid out on the herein clauses;
- e) that it will notify the data transferor of which individual within its organization will handle personal data processing enquiries and that it will collaborate with the transferor, with the data subjects and with the supervisory authority in good faith and that it will review such enquiries within a reasonable timeframe;
- f) that it will provide proof of possessing the financial means sufficient for fulfilling its obligations as laid out in clause III (inclusive of insurance) on request of the data transferor;

- g) that in response to a legitimate request by the transferor and upon reasonable notice and during office hours, it will enable it (and other independent or unbiased inspection agents or auditors appointed by the transferor who have not been unjustifiably challenged by the receiver) to conduct a review, audit and/ or certification of hardware used to process data and the files and documents related to data processing to check for their compliance with the guarantees and the undertakings laid out in the herein clauses. Such a request must be supported by a confirmation or approval of a legal or supervisory body of the data receiver's country which shall obtain such confirmation or approval within a reasonable timeframe;
- h) that it will process personal data to the best of its abilities in compliance with:
1. the data protection regulations of the transferor's country or
  2. appropriate regulations<sup>2</sup> of every Decision as issued by the Commission pursuant to Article 45 section 1 of GDPR, if the data receiver meets the appropriate provisions of such an authorization and operates in a country where the regulations apply, but is not subject to such authorizations or decisions pertaining to personal data protection<sup>3</sup>, or
  3. the rules on the transfer of personal data as laid out in Attachment 4.

The data receiver may choose one of the above options within [10] working days from the date of an agreement with the data transferor. If no choice is made by the data receiver, it is understood that the safeguards laid out in point 1 above shall apply {and} that it will not disclose or transfer personal data to a data controller from outside the European Economic Area (EEA) unless it notifies the data transferor of this and:

1. such country's data controller will process personal data in compliance with the Commission's adequacy decision as to the third party country, or
2. the third party country's data controller signs the herein clauses or another data transfer agreement as approved by an appropriate EU authority, or
3. the data subjects, following receipt of notice about the purpose of such a data transfer, categories of data receivers and the fact the receiver country may have different data protection standards in place, will have the right to object, or
4. data receivers have expressed explicit consent to the further transfer of sensitive data.

### III. Third Party Liabilities and Rights

- a) Parties will be mutually liable to one another for damages which occur as a result of the regulations set out in these clauses being breached. This mutual party liability is limited to actual damages. In particular, the possibility of compensation for harm suffered (e.g. compensation aimed at penalizing a party for its offensive behavior) is hereby excluded. Each

<sup>2</sup> „Appropriate regulations” shall refer to the regulations stemming from all permits and decisions with the exception of secondary legislations accompanying such permits or decisions.

<sup>3</sup> Nevertheless, the provisions of point 5 of Attachment A regarding the right to access, rectify, remove and object to processing must be applied if this option is selected and shall take priority over all other comparable provisions of the Commission.

party shall be liable before the data subject for damages which arise as a result of it having breached the rights of third parties as outlined in these clauses. This does not exclude liability of the data transferor stemming from data protection laws it is subject to.

- b) Parties agree that the data subject is entitled as a beneficiary - a third party – to apply the provisions of the herein clause and of clause I, items: b), I item d), I item e), II item a), II item c), II item d), II item e), II item h), II item i), III item a), V, VI item d) and VII to the data receiver and transferor if they should be in breach of the contractual obligations which apply to the subject's personal data. The laws of the data transferor's country shall become applicable for this purpose. On matters where a breach of provisions by the receiver is identified, the data subject must first approach the data transferor with a request it undertake appropriate steps to exercise its rights as to the actions it is entitled to take with regard to the data receiver, and if the data transferor fails to undertake such steps within a reasonable timeframe (within one month under ordinary circumstances), the data subject may pursue its rights directly with the data receiver. The data subject has the right to directly pursue his/ her rights with the data transferor who has failed in his obligation to establish whether the data receiver would be able to comply with the legal obligations as laid out in the herein clauses (the burden of proof that appropriate steps had been taken in this regard rests with the data transferor).

#### **IV. Law Herein Clauses Fall Under**

The applicable law which these clauses fall under is the law of the data transferor's country, with the exception of the laws and regulations related to the processing of personal data by the data receiver under point II item h) of the herein clauses which shall apply only if the data receiver so decides.

#### **V. Settlement of Disputes with Data Subjects or Supervisory Authority**

- a) In the event of disputes or claims for damages in connection with the processing of data between the data subject or the supervisory authority and each of the parties or both of the parties, parties will notify one another of the dispute or claim and shall collaborate to settle the dispute amicably within a reasonable timeframe.
- b) The parties hereby agree they will take part in every publicly available non-binding mediation process initiated by the data subject or the supervisory authority. Parties may opt to participate in mediation procedures remotely (over the phone or another electronic communication means). Furthermore, the parties agree they will give consideration to participating in other dispute resolution, arbitration or mediation procedures aimed at settling a personal data protection-related dispute.
- c) Each party shall fall under the jurisdiction of the court or the supervisory authority appropriate for the data transferor's country. The court's or the authority's verdict shall be considered final and cannot be appealed against.

## VI. Notice

- a) In the event when the data receiver is in breach of the obligations under these clauses, the transferor may temporarily halt the transfer of data to the receiver until such breach ceases or the agreement is dissolved.
- b) In the event when:
  - 1. data transfer to the receiver has been temporarily halted by the transferor for a period exceeding one month under item a),
  - 2. fulfillment of obligations under these clauses by the data receiver would cause it to breach obligations under the laws or regulations in effect in the country the data is being transferred to,
  - 3. the data receiver severely or persistently breaches any of the guarantees or provisions laid out in the herein clauses,
  - 4. a final verdict is delivered by an appropriate court or a supervisory authority of the data transferor's country, not subject to appeal, about the data transferor or receiver being in breach of the provisions of the herein clauses or,
  - 5. an application is filed for the appointment of an administrator or the liquidation of the data receiver, regardless of whether the receiver is an enterprise or a natural person, which is not rejected within the timeframe foreseen for such applications, a liquidation order is issued, a receiver is appointed to deal with any part of the estate, a receiver in bankruptcy is appointed – if the data receiver is a natural person, a process is put into place leading to a settlement or a similar legal process takes place, the transferor may, at no harm to its other obligations toward the receiver under these clauses, terminate these clauses and notify the supervisory authority accordingly.

In instances as spoken of in points 1, 2 or 4, the data receiver may also terminate the herein clauses.

- c) Each party may terminate these clauses if:
  - 1. The Commission issues an adequacy decision under Article 45, Section 1 of GDPR (or under text that supersedes it) in relation to the country (or its industry) to which data is transferred or in which data is processed by the receiver, or
  - 2. GDPR (or text that supersedes it) will be directly applied in that country ,
- d) Parties agree that the termination of the herein clauses at any time, for any reason and due to any circumstances [with the exception of termination under clause VI c)] does not exempt from obligations as imposed by the clauses and/ or the terms and conditions of processing of the transferred data.

## VII. Amendments To Clauses

Parties cannot amend the herein clauses with the exception of updates to all information contained in Attachment B, in which case, if required, parties will notify the supervisory authority of this fact. This does not exclude the possibility of the parties adding other commercial clauses.

### VIII. Description of Data Transfer

Details of personal data transfer are provided in Attachment B. Parties agree that Attachment B may contain confidential business information which they won't disclose to third parties unless required by law or by an order of an appropriate regulatory or government agency under point I, item e) of the herein clauses.

Parties may draw up additional attachments about additional data transfers which they will submit to the supervisory authority when necessary. As an alternative approach, Attachment B may cover multiple data transfers.

## ATTACHMENT A

### PRINCIPLES OF DATA TRANSFER

1. Restricted purpose: personal data may be processed and then used or transferred exclusively for the purposes outlined in Attachment B or once consent is obtained to such processing by the data subject.
2. Data quality and proportionality principle: data must be true and updated when needed. Data must be appropriate and not go beyond what's needed to accomplish the purposes for which they have been transferred and are being processed.
3. Transparency: the data subject must be given information necessary to ensure reliable data transfer (such as processing and transfer purpose), provided this information hasn't already been given by the data transferor.
4. Safeguards and confidentiality: the data controller must undertake technical and administrative measures to ensure a level of safeguards appropriate to counteract the risks which occur during processing such as accidental or unlawful damage or accidental loss of data, modification, unlawful disclosure or access to data. No individual acting on authority of the data controller, including individuals who have been entrusted with processing, may process data in a manner other than that which complies with the data controller's instructions.
5. Rights of data subjects (the right to information and access to data, the right to have the data corrected and removed, to have its processing restricted, the right to data transfer and the right to object to continued processing):
6. Pursuant to Article 12 of GDPR, the data subject should be provided with access, whether directly or via a third party, to all the personal data that pertains to it, with the exception of circumstances when the data subject abuses this right by frequent and unjustified, repetitive or systematic requests for access to data or when the laws of the transferor's country do not make it mandatory to grant access to such data. Pursuant to consent from a supervisory authority, the data subject may not be granted the right to access the data if such access were to seriously infringe on the legitimate interests of the data receiver or other organizations dealing with the data receiver, and provided such a move would not violate the fundamental rights and freedoms of the data subject. The source of personal data does not need to be disclosed if this does not prove possible in spite of legitimate steps having been undertaken or if this were to violate the rights of other persons.
7. The data subject must have the right to correct or remove data from the database if these prove imprecise or are not processed in line with the rules as listed in this Attachment. If there are important reasons to doubt such a request is legitimate, the organization may demand an explanation prior to correcting, rectifying or removing data from the database. It is not necessary to notify the third parties who have been disclosed the amended, corrected or removed data if such notification were to require excessive efforts to be undertaken. The data subject should also have the right to object to data processing for legally justifiable reasons stemming from the data subject's particular circumstances.



8. The burden of proof of the legitimacy of the refusal to grant access to data rests with the data receiver, and the data subject shall always have the right to appeal this refusal to the supervisory authority. Sensitive data: the data receiver must undertake extra measures (for example safety measures) necessary to ensure sensitive data are protected in line with its obligations under point 2 of the above clause.
9. Data used for direct marketing purposes: when data is processed for direct marketing purposes, effective procedures should be put into place to ensure the data subject can prohibit the use of data for these purposes at any time.
10. Automated decision-making: under these clauses, the phrase "automated decision-making" shall refer to decisions by the transferor or receiver which lead to legal implications for the data subject or have substantial impact on the subject's circumstances, and which are based exclusively on automated data processing used to assess some personal features, such as professional achievement, credit rating, reliability, behavior, etc. The data receiver must not use automated decision-making with regard to the data subject, except when:
  - a) such decisions are made by the data receiver while entering into or performing under an agreement with the data subject, or
  - b) the data subject has the opportunity to discuss the implications of automated decision-making with a representative of the party who has made such a decision or present his/ her point of view to the other party in another manner, or
  - c) such a decision is required by law in the receiver's country.



## ATTACHMENT B

### DESCRIPTION OF DATA TRANSFER

#### Data Subjects:

Personal data being transferred pertains to the following categories of individuals:

- 1) individuals who take part in the process of delivering services as provided by the data receiver, including workers, co-workers and individuals acting for and on behalf of the transferor of the data of its sub-contractors or customers,
- 2) consignors and consignees of shipments and individuals acting for and on their behalf, the extent to which the transfer of data of these individuals to a third party country may not be accomplished while maintaining the safeguards other than the herein clauses, under Articles 44-49 of GDPR, and specifically when one of the exceptions as listed in Article 49 Section 1 items b, c and e of GDPR cannot be used as the grounds for such a transfer, i.e.:
  - b) when the transfer is necessary to perform under an agreement between the data subject and the controller or to enforce precontractual measures undertaken at the request of the data subject;
  - c) when the transfer is necessary to enter into or perform under an agreement made in the interest of the data subject between the controller and another natural or legal person; [...]
  - e) when the transfer is necessary to establish, pursue or protect against claims for damages.

#### Data Transfer Purpose(s)

Data transfer is necessary for the following purposes:

To deliver services provided by the receiver or to potentially establish, pursue or defend against claims for damages after the services have been performed.

#### Data Categories:

The transferred personal data pertain to the following data categories:

First and last name, telephone number e-mail address, ID card data, address.

#### Receivers:

The transferred data may be disclosed to the following receivers and receiver categories only: entities part-taking in the process of contracting and delivering services for and on behalf of the data receiver, entities part-taking in a potential process of establishing, pursuing or defending against claims for damages.

#### Sensitive Data:

Not applicable.