PROCESSING AGREEMENT under Art 28 GDPR

1. Subject-matter of the agreement

a) Österreichische Post AG (Post) provides, for the purpose of shipping preparation to their customer (Controller) / the customers vicarious agent the Post – Labelcenter (PLC).
When this labelling system is used by the customer (Controller) / the customers vicarious agent, Post is in the role of the Processor according to the GDPR.
For purposes of this Agreement "personal data" shall mean such personal data which the Controller provides to the Processor under the agreement described above in more detail and/or which is to be processed by the Processor under such agreement.

b) Categories of personal data and categories of data subjects as set out in Annex 1 are processed.

2. Tasks of the Processor

a) The Processor undertakes to process any personal data and processing results solely as ordered by the Controller in writing (email being sufficient).

b) The Processor may not disclose to third parties any personal data of the Controller without the Controller's written consent.

c) Where required by statutory provisions, the Processor shall give immediate advance notice to the Controller.

d) Any transfer of personal data to third parties the Processor need not perform by law shall require a written order by the Controller (email being sufficient).

e) The Processor may process any personal data for the Processor's own purposes only subject to the Controller's prior written consent (email being sufficient).

f) The Processor agrees to maintain data secrecy and states with legally binding effect that the Processor has bound all parties entrusted with processing tasks, before they start work, to keep personal data confidential or that such parties are subject to a reasonable statutory confidentiality obligation.
The Processor has bound all parties entrusted with processing tasks to keep confidential any personal data which is entrusted or made available to them solely due to their work, irrespective of any other statutory confidentiality obligations, unless there is any lawful reason to transfer/disclose such data.
The confidentiality obligation of all parties entrusted with processing tasks shall remain valid even when they have completed their work and leave the Processor's business.

g) The Processor states with legally binding effect to have taken all necessary measures to ensure the security of processing under Art 32 GDPR.
The Processor guarantees to have taken and to take in future any technical and organisational measures described and selected in Annex 2 and appropriately reflecting the risk involved in order to protect any personal data against any fortuitous or unlawful destruction or any loss to ensure such data is properly processed and not available to unauthorised third parties. The Processor undertakes to maintain the state

of the art of such technical and organisational measures and to update and/or adjust such measures to reflect any technical progress and/or change in risks.

h) The Processor shall ensure that the Controller can satisfy at any time within statutory time-limits the rights of the data subject under Chapter III GDPR (information, access, rectification and erasure, data portability, right to object and automated individual decision-making), taking into account the Austrian Federal Act on the Protection of Individuals in the Processing of Personal Data (Data Protection Act, as amended). The Processor shall make available to the Controller all necessary information and shall use his best efforts to assist the Controller in satisfying any related obligations.
If a request asserting rights of the data subject is addressed to the Processor and such request shows that the requesting party erroneously believes that the Processor is the Controller of the processing activities carried out by the Processor on behalf of the Controller, the Processor shall immediately forward such request to the Controller and give notice thereof to the requesting party, disclosing the date of receipt of the request.

i) The Processor shall use his best efforts to support the Controller in complying with the obligations referred to in Art 32 to 36 GDPR (data security measures, notifications of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment, prior consultation).

j) The Processor agrees to provide the Controller with such information as required to monitor compliance with the obligations referred to herein.
On request by the Controller, the latter shall be provided on a case-by-case basis with the statement binding any individuals entrusted with processing to maintain data secrecy.

k) As regards the processing of personal data made available by the Controller, the latter shall be granted the right to review, or to have reviewed by qualified employees subject to confidentiality or by any individual subject to a duty of professional secrecy (certified court expert, etc.), the proper processing of data by the Processor, subject to prior notice of at least 30 workdays (excluding Saturdays) and at the Controller's own cost and expense. Such review may be performed during regular office hours and in agreement with the Processor's data protection officer or any other individual responsible for data protection.

l) Once the Processor has completed his work, the Processor shall hand over to the Controller all processing results and documents containing personal data hereunder. This shall not affect the storage of any personal data provided to the Processor and any processing results, insofar and as long as the Processor is required to warrant for his services.
After the expiration of the warranty period, the Processor shall erase all personal data hereunder or, at the Controller's request, safely store such data before erasing them, especially if the Processor is not required to continue to store personal data under mandatory laws.
The Processor shall confirm the erasure of data in writing at the Controller's request.
If the Processor processes personal data in a special technical format, the Processor, after completion of his work, shall deliver the personal data in such format or, at the Processor's request, in the format in which he received the personal data from the Controller or in any other customary format.

m) Liability shall be based on statutory provisions and any liability provisions under data protection laws as set forth in the main service agreement.

Liability shall not exceed a year's order volume of the main service agreement pursuant to Section 1a) above, unless such agreement or the law includes a more beneficial provision for the Processor.

3. Sub-processors

a) The Processor may use sub-processors. The Processor shall inform the Controller of his intention to use sub-processors in such timely manner that the Controller may prohibit such use.
The foregoing shall not include any ancillary services the Processor is using, e.g. postal / transport / telecommunication services or services to maintain / service data carriers and data processing equipment.

b) The Processor shall make the necessary agreements as set forth in Art 28 (4) GDPR with the sub-processor. The Processor shall ensure that the sub-processor enters into the same obligations imposed upon the Processor hereunder. The transfer of such obligations shall be proven to the Controller upon request.

c) If the sub-processor does not satisfy his data protection obligations, the Processor shall be liable to the Controller for compliance with the sub-processor's obligations.

d) The Controller shall issue his consent to use the sub-processors referred to in Annex 3.

4. Term

The term hereof depends on the agreement referred to in Section 1a).

5. Miscellaneous

a) All disputes arising from and in connection with this Agreement shall be governed by and construed in accordance with Austrian law, without giving effect to the UN Sales Convention and any conflict of law rules. All disputes shall be referred to the court having subject-matter and local jurisdiction for 1030 Vienna.

b) Only written agreements shall be binding; there are no oral side agreements. Any amendment to and modification of this Agreement, including any waiver of the written form requirement, shall be made in writing to be valid.

c) All rights and obligations hereunder shall transfer to any successor of either party.

d) The parties agree to keep confidential the execution as well as the terms and conditions hereof, unless this Agreement includes any provision to the contrary or any statutory disclosure obligation applies.

e) The Controller agrees that (i) his legal representatives, employees and any subcontractor used and/or hired will comply with all applicable statutory provisions in relation to anti-corruption regulations, and (ii) he will take appropriate measures to ensure compliance with any anti-corruption regulations. Notwithstanding any other rights of rescission and termination, any violation of anti-corruption regulations shall entitle the Processor to give notice of extraordinary termination hereof with immediate effect and to assert any claims for damages.

f) If any term hereof is or becomes invalid or ineffective, the parties will agree on a valid and/or effective term which closest reflects the economic effect of the invalid and/or ineffective term.
The invalidity or ineffectiveness of any term hereof shall not affect the validity or effectiveness of the entire Agreement.

g) This Agreement will be executed in two originals. Either party shall receive one original.

h) Annexes 1, 2 and 3 hereto shall form integral parts hereof.

Annex 1 - Categories of personal data and data subjects

a) The following categories of personal data are processed

x Personal details (first and family name, academic degree, date of birth, family status, sex, citizenship, etc.)

x Contact details (phone number, email address, fax)

x Address details (postal address)

b) Personal data concerning the following categories of data subjects is processed

x Customers

Annex 2 - Technical - organisational measures

(All measures to be taken must be defined specifically, which is why the Processor ticked all applicable boxes)

1) CONFIDENTIALITY

Access control - protection against unauthorised access to data processing equipment

☒ Alarm system	☒ Security staff
☒ Keys	☒ Video surveillance of access paths
☒ Safety locks	☒ Identity check at the entrance
☒ Authorisation passes	☒ Recording of visitors

Access control - protection against unauthorised system use

☒ Role-based allocation of user rights	☒ Security Incident Management & Security Operation Centre
☒ Secure passwords/password policy	☒ Automatic lock mechanisms/screen lock

Access control - protection against unauthorised reading, copying, modifying or removing within the system

☒ Authorisation concept "need to know basis"	☒ Safe storage of data carriers
☒ Recording of any access	☒ Pseudonymisation
☒ Encryption of data carriers	☒ Firewall
☒ Rights management by system administrators	☒ Disposal of data carriers in compliance with data protection laws and recording
☒ Classification scheme for data	☒ Standard processes when employees are transferred/leave the company
☒ VPN technology	

2) INTEGRITY

Transfer control - protection against unauthorised reading, copying, modifying or removing upon transfer

☒ Encrypted data transfer	☒ Documentation of data recipients
☒ Secure transport containers	☒ Antivirus software
☒ Encryption of data carriers	☒ Overview of regular retrieval and transfer processes
☒ Intrusion detection system	

Entry control - identification whether and by whom personal data was entered, modified or removed in data processing systems

☒ Recording	☒ Entry validation
☒ Document management	

3) AVAILABILITY AND RESILIENCE

Availability control - protection against destruction and loss of data

☒ Backup & restore tests	☒ Fire and smoke alarms
☒ Uninterrupted electricity supply	☒ Recovery concept/recovery plan
☒ Redundancy concepts/emergency plan	☒ Air-conditioning
☒ Time limits for erasure	☒ Channels of communication and emergency plans

4) PROCESSES FOR SUPERVISION, ASSESSMENT AND EVALUATION

☒ Data protection management	☒ Regular employee training
☒ Security management	☒ Security checks on infrastructure and application level

5) OTHER

☒ Data protection by design and by default	☒ Right to give instructions
☒ Unambiguous contracts	☒ Formalised order management
☒ Careful selection of service providers	☒ Supervision / audit right
☒ Checking and documentation of security measures	☒ Physical/logical separation of data
☒ Requirement to comply with data secrecy (e.g. employees)	☒ Separation of productive and test system

Annex 3 - Sub-processors

The Processor may use the following sub-processors:

Name	Address	Type of activity
ondot solutions GmbH	Brown-Boveri-Straße 8/1, 2351 Wiener Neudorf	Software Development Customer Support
SVISS GmbH | IT-Service Management Solutions	Industriestraße 24 – 2A A-7400 Oberwart	Customer Support