

## DATA PROCESSING ADDENDUM

Aktsiaselts Eesti Post, registration code 10328799, with its registered office at Pallasti 28, 10001 Tallinn, Estonia (the "Controller" or "Omniva"), duly identified in the Service Agreement signed between the Courier and Omniva for Crowd Delivery services (the "Main Agreement"), the one hand,

The Courier, (the "Processor"), duly identified in the Main Agreement, on the other hand,

each separately hereinafter also referred to as a Party and together as the Parties, have entered into this Data Processing Addendum (hereinafter referred to as the "DPA") on the following terms:

### 1. PURPOSE

1.1. Processor provides a service to the Controller through the Main Agreement and processes the personal data of the Controller's clients, as a processor under the Applicable Data Protection Legislation. For this reason, the Parties hereby sign the DPA to govern the processing of personal data.

1.2. The DPA is an integral part of the Main Agreement and by signing the Main Agreement the Parties attested that they are also signing this DPA.

1.3. The content and duration of the processing of personal data, the nature and purpose of the processing, the type of personal data and the categories of data subjects are specified in Annex 1 to this DPA.

### 2. DEFINITIONS

2.1. Third Party - any natural or legal person who is not a Party to the DPA or to the Main Agreement and all such employees and/or service providers of the Parties who are not directly and immediately engaged in the performance of the works and provision of the services agreed in the Main Agreement.

2.3. Applicable Data Protection Legislation - means any applicable legislation relating to data protection and security, including the Directive on privacy and electronic communications (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector) and the General Data Protection Regulation (Regulation 2016/679 of the European Parliament and of the Council of 27 June 2016 on 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 (hereinafter referred to as the GDPR), and any amendments, replacements or extensions thereof (collectively "EU legislation"),

any mandatory national laws implementing EU legislation, and any other mandatory data protection or data security directives, laws, regulations and decisions in force at the relevant time and relevant EU Member State laws.

2.4. The terms "processing of personal data", "personal data", "data subject", "personal data breach" have the meaning given to them in the GDPR.

## 3. REQUIREMENTS FOR THE PROCESSING OF PERSONAL DATA AND THE RIGHTS AND OBLIGATIONS OF THE PARTIES

### 3.1. Rights and obligations of the Controller

3.1.1. The Controller agrees and confirms that its processing of personal data in the performance of the DPA is lawful in accordance with the Applicable Data Protection Legislation.

3.1.2. The Controller shall provide the Processor, upon request, with the information necessary for the Processor to fulfil its obligations under the DPA.

3.1.3. The Controller shall ensure that the processing of personal data complies with the requirements of the Applicable Data Protection Legislation and shall put in place organisational, physical, and technical security measures for the protection of personal data that comply with the requirements of the Applicable Data Protection Legislation.

3.1.4. The Controller has the right to check regularly (including before entering into or commencing performance of the Main Agreement) the compliance of the processing of personal data by the Processor with the Applicable Data Protection Legislation, as well as the requirements of the Controller's regulations, including the existence of appropriate security measures. When carrying out the audits, the Controller shall take into account the business activities of the Processor and shall carry out the audits in a manner that minimises the impact on the Processor and its day-to-day operations.

3.1.5. The Controller has the right to require the Processor to complete and submit a written self-assessment form to verify compliance with the Applicable Data Protection Legislation at any time prior to the conclusion of the Main Agreement and during the term of the Main Agreement.

### 3.2. Rights and obligations of the data Processor

3.2.1. The Processor shall ensure that it and its authorised persons do not process personal data to a greater extent or for purposes other than those necessary for the fulfilment of the requirements of the Main Agreement, this DPA, and the Applicable Data Protection Legislation.

3.2.2. The Processor undertakes to comply with the requirements imposed on the Processor by this DPA, the Applicable Data Protection Legislation, as well as by the regulations, instructions, and orders of the Controller.

3.2.3. The Processor undertakes to ensure the proper protection of the rights of the data subjects in accordance with the Applicable Data Protection Legislation, the DPA and the instructions, directions and relevant regulations issued by the Controller.

3.2.4. The Processor undertakes to comply with all instructions given by the Controller in relation to the provision of the service. The Processor undertakes to inform the Controller without delay, but no longer than in 10 days, if, in the opinion of the Processor, an order or instruction given by the Controller would lead to a breach of the Applicable Data Protection Legislation.

3.2.5. In addition to the requirements of Article 32 of the GDPR, the Processor must comply with the following security requirements and obligations:

- Not extract, transfer, screenshot, transcribe nor in any way create copies of data (including but not limited to personal data) provided to the Processor by the Controller, including those shared through the application used for the provision of the services or other official channels agreed in the Main Agreement;
- Not share access to the application and other official channels for the provision of the services nor to the data contained therein to any person not authorised by the Controller;
- Keep its credentials to the application and any other channel or system used for the provision of the services confidential and secure, being prohibited to share those to any unauthorised person;
- Avoid using outdated third-party software or operational systems for the provision of the services. Updates must be installed promptly;
- Install promptly updates of the application made available for the provision of the services;
- Ensure that any devices used for the provision of the services have malware protection and keep the highest level of security configurations available in those devices (such as enabled password/ face ID).

3.2.6. The Processor also undertakes to independently implement organisational, physical and technical security measures for the protection of personal data which comply with the requirements of the Applicable Data Protection Legislation. In implementing security measures, the

Processor shall take into account the nature, purpose, context and scope of the processing.

3.2.6.1. At the request of the Controller, the Processor undertakes to inform the Controller of the additional security measures taken to protect personal data and any changes thereto.

3.2.7. The Processor undertakes to provide the Controller, without charge, with all the information and documentation and to provide all the assistance necessary for the Controller to comply with all the requirements of the Applicable Data Protection Legislation and to demonstrate compliance with those requirements in respect of the personal data relating to the DPA, as well as to allow and facilitate audits by regulatory and/or supervisory authorities or by the Controller or its representative. The Controller may also request the Processor to carry out security audits regarding the processing of personal data at any time, and the Processor must comply with the requests of the Controller regarding such audits, including presenting the results of such audits, in the format specified by the Controller, within 10 days of the request. If an audit reveals a breach of this DPA or of the security requirements by the Processor, including where the breach is caused by its affiliates, consultants, sub-processors or other agents, the Processor shall bear the costs of the audit of the Controller.

3.2.8. The Processor undertakes to keep and keep available up-to-date records of the processing operations in accordance with Article 30 of the GDPR, and to provide the Controller, upon the Controller's request and without undue delay, with the documentation provided for in this Clause, in order to enable the Controller to comply with the Applicable Data Protection Legislation.

3.2.9. The Processor undertakes to respond to the Controller's requests and to provide all relevant information requested in the request in relation to compliance with the requirements of the agreement within 10 days of receipt of the request.

3.2.10. The Processor undertakes to keep personal data processed and disclosed through the Controller separate from the data of third parties and its own data.

3.2.11. The Processor undertakes to keep the personal data confidential (i.e. to ensure that the data cannot be accessed by unauthorised persons, including the Processor's employees who are not involved in the performance of the Main Agreement or this DPA) and to ensure that all persons who are authorised to process personal data are informed of the confidential nature of the personal data, have received appropriate training on their obligations and have assumed an obligation of confidentiality or are subject to an appropriate legal obligation of confidentiality.

3.2.12. The Processor undertakes to notify the Controller without undue delay, but not later than

within 24 hours, of any breach of the Agreement and of the Applicable Data Protection Legislation (including cases of suspected or confirmed unauthorised access of the application or of the devices utilized for the provision of the services), as well as of any complaint lodged with the Processor regarding a breach of the data protection legislation by the Processor, and, if such situations arise, to resolve them as soon as possible in order to avoid further damage and to mitigate the effects of the incident. In the event of a personal data breach, the data Processor shall immediately take appropriate measures to remedy the breach, mitigate its adverse effects and prevent future breaches.

3.2.13. The Processor undertakes to transmit the notification under point 3.2.12 to [privacy@omnivagroup.com](mailto:privacy@omnivagroup.com), attaching the personal data breach notification to the notification:

- the time of the infringement;
- the circumstances of the infringement;
- why the infringement happened;
- the number of personal data records affected by the breach;
- what personal data are affected by the breach;
- the number of people affected by the infringement;
- which categories of persons are concerned by the infringement;
- possible consequences for the persons affected by the infringement;
- the measures taken to address the breach, mitigate the adverse effects and prevent future breaches;
- the cross-border impact of infringements.

3.2.14. Only in a situation where the Processor is involved in such a personal data breach that involves personal data of several different Controllers (including on behalf of Omniva) and Article 33 of the GDPR requires that such a breach be notified to the Data Protection Inspectorate, the Controller authorises the Processor to submit a breach notification to the Data Protection Inspectorate also on behalf of Omniva. The notification of the breach shall, inter alia, state that the breach notification is also submitted on behalf of Omniva. The Processor undertakes to inform the Controller in advance of the intention to lodge of such an infringement report.

3.2.15. The Processor undertakes to inform the Controller without delay if the Processor is the subject of proceedings which may give rise to a claim for compensation or a fine under the Applicable Data Protection Legislation. In the event of the initiation of such proceedings, the Processor shall: (a) provide the Controller with the details (including the specific allegations relating to the infringement); (b) provide the Controller with the information and assistance requested by the Controller; and (c) not prevent the Controller from

actively participating in the proceedings (through legal assistance at its own expense)

3.2.16. If a data subject, a supervisory or government authority (e.g. the Data Protection Inspectorate) or any other third party requests the Processor to process personal data on the basis of an contractual relationship with the Controller, the Controller shall direct the data subject's request to the Controller's contact [privacy@omnivagroup.com](mailto:privacy@omnivagroup.com). The Processor shall not disclose personal data or other information concerning the processing of personal data without the prior written consent of the Controller, unless the Processor is required to disclose such data under mandatory European Union or Member State law. In the latter case, the Processor shall promptly inform the Controller of the request to the extent permitted by law, but in any case before responding to the request.

3.2.17. The Processor undertakes not to use sub-processors for the processing of personal data, not to transfer personal data to third parties, or to give access to or involve third parties in the processing of personal data without the prior written consent of the Controller. Where such consent is given, the transfer of personal data by the Processor shall be conditional upon the imposition on the relevant third party of the same data protection obligations as set out in the Agreement prior to the transfer of the personal data, and the Processor shall also be liable for the third party's compliance with and breaches of those obligations. At this moment no sub-processor has been authorised.

3.2.18. The Processor processes personal data only within the European Union or the European Economic Area and does not transfer the data outside the European Union or the European Economic Area, nor does it provide access to the data to persons located outside the aforementioned area. The software, its components and interfaces (including mass mailing software) used by the Processor on behalf of the Controller for the processing of personal data must process the personal data in the European Union, in a country/company that is a agreeing party to the Agreement on the European Economic Area or in a country/company with an adequacy decision of the European Commission. In the case of the use of a sub-processor in a third country with an inadequate level of data protection within the meaning of Chapter V of the GDPR, the Processor must ensure and demonstrate that the sub-processor complies with the requirements of Chapter V of the GDPR (in particular, that it has concluded standard data processing clauses with the European Commission, that it has carried out a cross-border data impact assessment (TIA) and that it has implemented additional safeguards (e.g. SCCs).

3.2.19. The Processor undertakes to return in the agreed form and/or destroy (at the choice of the

Controller) all personal data processed on behalf of the Controller at the expiry or termination of the Main Agreement. The Processor shall provide evidence to that effect at the request of the Controller.

#### **4. LIABILITY**

4.1. In the event of non-performance or improper performance of the obligations provided for in the DPA, the Party shall be liable in accordance with the procedure provided for in the legislation and the Main Agreement.

4.2. The Party that has suffered damage as a result of a breach of the DPA has the right to file a claim for compensation of the damage caused to the Party that caused the damage.

4.3. The Party in breach of the DPA undertakes to pay the claim for damages to the other Party within 30 (thirty) calendar days from the date of receipt of such claim.

#### **5. VALIDITY OF THE AGREEMENT**

5.1. The Agreement shall enter into force from the moment of signature of the Main Agreement and shall remain in force until the expiry or termination of the Main Agreement with the Processor. Termination of the Main Agreement shall not terminate the obligation of the Processor to respect the confidentiality and security obligations of personal data.

5.2. The Controller may alter the DPA upon publication of the amended version in the <https://www.omnivagroup.com/policies/> Data Processing Addendum (Crowd Delivery) and communication to the Processor. The Processor shall have 30 days to oppose the modification by the Controller. In the event of absence of declaration by the Processor, the new DPA shall come into force

5.3 The Agreement shall be governed by law of the Main Agreement.

### **ANNEX 1 TO THE DPA - DESCRIPTION OF PERSONAL DATA AND THEIR PROCESSING**

#### **1. Purpose, content and nature of the processing of personal data**

The Processor processes personal data for the Controller in connection with the service referred to in Clause 1.2. of the DPA (i.e., provision of Crowd Delivery services under the Main Agreement).

##### **1. Types of personal data**

*The following categories of personal data are processed under the Agreement:*

- Identity code;
- First and last name, alias, username;
- Identity document number;
- Postal delivery code;
- Data related to the use of the postal service;
- Data relating to the use of a financial service;
- Date of birth;
- E-mail address;
- Telephone number;

##### **2. Categories of data subjects**

The processing concerns the following categories of data subjects:

- Customers of the Controller;
- Customers of the Controller's business clients;

##### **3. How the data is processed**

*Processor will receive information regarding the aforementioned data subjects through an application managed by the Controller in order to be able to retrieve and deliver parcels on behalf of the Controller. Processor may not transfer the data received to any other environment, format or medium. Data may not be processed in any other way.*

##### **4. Duration of processing of personal data**

*Processor will process data of a certain data subject solely within the duration of its delivery service involving that data subject.*

## PERSONAL DATA BREACH NOTIFICATION GUIDE FOR OMNIVA PROCESSORS

### 1. Purpose of the guide

Omniva and the Processor have concluded a Data Processing Addendum (“DPA”), under which the Processor is obliged to inform Omniva of any personal data breach that has occurred. The purpose of this guide is to inform Omniva's Processors of their obligations under the Applicable Data Protection Legislation and the Agreement in relation to the detection, handling and notification of personal data breaches.

### 2. Definitions

For the purposes of this guide, the following definitions apply:

**Data subject** - a natural person, i.e. a person whose personal data is processed by an authorised Processor.

**Supervisory Authority** - Data Protection Inspectorate.

**Breach** - a personal data breach under the GDPR.

**GDPR** - General Data Protection Regulation of the European Union.

**Processor** - means the Processor provided for in the Agreement.

Other terms used in the Guide have the meaning given to them in the Agreement or the GDPR.

### 3. Personal data breaches

A breach is a security incident that results in the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There are three types of breaches:

- 3.1. Breach of confidentiality - unauthorised or accidental disclosure of or access to personal data. For example, where private customers' home addresses and email addresses become publicly available online due to a technical error or human error.
- 3.2. Breach of integrity - unauthorised or accidental alteration of personal data.
- 3.3. Breach of availability - temporary denial of access to personal data, or where personal data have been permanently lost or destroyed. For example, where data has been accidentally deleted and cannot be recovered, or where the key to securely encrypted data has been lost, etc.

The infringement may be linked to different combinations of the listed types at the same time.

The Processor is obliged to ensure that its employees are trained and informed about the infringements and their obligations.

Under the GDPR, Omniva has an obligation to notify certain breaches without delay (in certain cases within 72 hours) to the supervisory authority and/or the data subject. In the event of a breach involving personal data held by the Processor, the Processor must notify Omniva in accordance with the DPA. Pursuant to Clause 3.2.14. of the DPA, if the personal data breach of the Controller concerns several different controllers, including AS Eesti Post, the Controller authorises the Processor to submit a breach notification to the Estonian Data Protection Supervisory Authority also on behalf of the Controller.

### 4. Notifying Omniva of an infringement

According to the Agreement, upon discovery or notification of a breach or potential breach, the Controller is obliged to:

-immediately, before reporting a breach, to take appropriate measures within its competence to minimise the potential damage caused by the breach.

For example, inform the person who has received an email that contains personal data in error that the email, together with the personal data it contains, must be deleted and that the processing of the personal data contained in the email is unlawful.

-immediately, but no later than within 24 hours, notify Omniva of the breach by contacting [privacy@omnivagroup.com](mailto:privacy@omnivagroup.com).

However, if the Processor is not sure whether a breach has occurred, but has reasonable grounds to suspect that a breach has occurred, the notification must still be forwarded to Omniva so that Omniva can analyse the case and, if necessary, provide guidance to the Processor.

The following information must be provided by the Processor upon registration of the breach:

- the date and time of discovery of the infringement,
- the time of the infringement,
- the circumstances of the infringement,
- when the Processor became aware of the breach,
- the consequence of the infringement,
- the types of personal data (e.g. name, personal identification number, address) affected,
- how many data subjects are affected by the breach,
- what categories of persons were affected by the infringement (e.g. Omniva employee, Omniva private customer),
- what the possible consequences of the breach are for the data subject,
- the measures taken to address the breach, mitigate the adverse effects and prevent future breaches;
- the cross-border impact of the infringement.

In the event that the Processor receives a breach request from supervisory authorities, a data subject or a third party, the Processor is obliged to notify Omniva of the request immediately via the contact email [privacy@omnivagroup.com](mailto:privacy@omnivagroup.com) and receive further instructions on how to deal with the request.

If you have any further questions, please contact Omniva at [privacy@omnivagroup.com](mailto:privacy@omnivagroup.com).

#### **5. Consequences of infringements**

A breach, if not addressed appropriately and in a timely manner, may result in physical, material and/or non-material harm to the data subject, such as:

- loss of control or restriction of your personal data,
- discrimination,
- identity theft or fraud,
- financial damage,
- reputational damage,
- loss of confidentiality of data protected by professional secrecy, etc.

Failure to address breaches appropriately and in a timely manner may result in Omniva and the Processor in particular in supervisory authority proceedings with legal consequences (e.g. injunction, warning, fine, etc.), reputational damage, damages claims by data subjects as well as Omniva's business customers