Roisender Data Processing Agreement

PLEASE READ THIS DATA PROCESSING AGREEMENT CAREFULLY. THIS DATA PROCESSING AGREEMENT GOVERNS THE TRANSFER AND PROCESSING OF PERSONAL DATA BY THE PROVIDER ON BEHALF OF THE USER AND IN CONNECTION WITH THE USERS USE OF THE ROISENDER SERVICE. BY SETTING UP AN ACCOUNT AND CLICKING [I AGREE] OR USING ANY OF THE ROISENDER SERVICES WHICH DO NOT REQUIRE REGISTRATION, YOU AGREE TO BE BOUND BY THE ROISENDER TERMS OF SERVICE AND THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, YOU MAY NOT ACCESS OR USE THE ROISENDER SERVICE.

PREAMBLE AND INTRODUCTORY REMARKS

This **Roisender Data Processing Agreement** and its **Annexes** (herein after: "**DPA**") reflects the parties' agreement with respect to the **Processing** of **Personal Data** by the **Provider** (as the **Processor**) on behalf of the **User** (as the **Controller**) in connection with the **Users'** use of the **Roisender Service**, whereby all bolded terms are further defined below.

This **DPA** is supplemental to, and forms an integral and indispensable part of the **Roisender Terms of Service** (hereinafter: "**Terms**" or "**Agreement**") published on www.roisender.com/terms, which apply to all websites and services that are represented by the **Roisender** (unregistered) trademark and govern the setting-up, use and access of the **Roisender Service** and the roisender.com website.

This **DPA** is effective from the moment that the **Provider** and **User** enter into the **Agreement** as described in point 1.1. of said **Agreement**.

If you do not agree to the terms and clauses of this **DPA** or the **Agreement**, you are not authorised to validly register an account with us as well as access or use the **Roisender Service** and the roisender.com website, and you must immediately stop doing so.

In case of any conflict or inconsistency between the terms and clauses of this **DPA** and the terms and clauses of the **Agreement**, this **DPA** will take precedence over the terms and clauses of the **Agreement** to the extent of such conflict or inconsistency.

Terms not otherwise defined in this **DPA** will have the meaning as set forth in the **Agreement**.

All enquiries regarding this **DPA** may be directed at data@roisender.com

1. THE APPLICATION OF THIS DPA

1.1. By setting up an account and clicking [I agree] or using any of the **Roisender Services** which do not require registration as described in point 1.1. of the **Agreement**, this **DPA** is deemed as validly concluded between:

- KOMPETENTNOST d.o.o., Žolgarjeva ulica 20, SI-2000 Maribor, Slovenia, EU, Company Registration Number: 6394329000, VAT ID Number: SI 83297286, the owner and supplier of the **Roisender Service** and the **www.Roisender.com** website (hereinafter: *"**we**"*, *"**us**"*, *"**our**"*, *"**Provider**"* or "***Processor***") who can be reached / dpo or through the messaging application on the aforementioned website,
- and **you** (hereinafter: *"**you**", "**your**"*, *"**User**"* or "***Data Processor***") the legal entity that shall be identified as the registered user of the **Service** when you, the duly authorised individual representing said entity, register an account (i.e. perform the actions from point 1.1. of the **Agreement** in the name the company you represent) is bound to the **Agreement** and this **DPA**. The aforementioned also relates to any and all **Permitted Users**, **Personnel** and **User Affiliates.**

1.2. Before your use of the **Service**, you are asked to dully review, understand and get acquainted with the content of both this **DPA** and the **Agreemen**t.

1.3. Any reference to this DPA includes its Annexes.

2. CHANGES

2.1. We may make changes to this **DPA** at any time by notifying you of the change by email or by posting a notice on the **www.Roisender.com** website. Unless stated otherwise, any change takes effect from the date set out in the notice. You are responsible for ensuring you are familiar with the last version of this **DPA**. By continuing to access and use the **Roisender Service** and the **www.Roisender.com** website from the date on which this **DPA** is changed, you agree to be bound by the changed **DPA**.

2.2. If you do not agree to the changes, you must notify us immediately whereby we shall proceed with terminating your account and ceasing any and all **Data Processing** and returning / destroying all **Personal Data** to you as per the applicable clauses of the **Agreement** and this **DPA**.

2.3. This DPA was last updated on 12.09.2022

3. INTERPRETATION

3.1. In this **DPA**:

Agreement (also called **Terms**) shall mean the **Roisender Terms of Service** published on https://www.Roisender.com/terms-of-service, which apply to all websites and services that are represented by the **Roisender** (unregistered) trademark and govern the setting-up, use and access of the **Roisender**

Service and the **www.Roisender.com** website and under which certain **Personal Data** needs to be processed in accordance with this **DPA**.
Applicable legislation shall mean but not be limited to the European Union's General Data Protection Regulation (2016/679) (hereinafter: ***"GDPR"***) as well as any and all applicable EU and national laws and other statutes, rules, regulations and codes, as they may apply to the use and the consequences of use of the **Roisender Service** by the **User** in the country where the **User** or his legal entity is established or operates or where the **End User** or other effected natural persons reside, as amended, replaced or superseded from time to time. **Applicable legislation** shall also mean but not be limited to any and all USA equivalents of such laws (e.g. the **California Consumer Privacy Act** (**CCPA**), the **Telemarketing and Consumer Fraud and Abuse Prevention Act**, the **Do-Not-Call Implementation Act**, the **Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003**, the **Children's Online Privacy Protection Act (COPPA)**, as well as relevant EU directives (e.g. the **Electronic Communications Directive 2002/58/EC** (the **ePrivacy Directive**), codes of conduct and industry standards (e.g. the **Cellular Telecommunications Industry Association (CTIA) Messaging Principles**), as amended, replaced or superseded from time to time.
Roisender Service (also called **Service**) shall mean the software program with the core functionality as described on the **www.Roisender.com** website, as the website is updated from time to time, whereby the software is the proprietary intellectual property of the **Provider** and is made available to you and your **Permitted Users** via the **www.Roisender.com** website or by way of download and integration of the **Roisender Plugin** application via the WordPress App Store:
Roisender Data Processing Agreement (also called **DPA**) shall mean this legal agreement that you shall simultaneously enter into together with the **Agreement** when performing the actions from point 1.1. of the **Agreement**, and under which the **Provider** shall be deemed as the **Processor** and you shall be deemed as the **Controller** of any and all **Personal Data** that shall be sent, transmitted or transferred to the **Provider** directly or through the use of the **Roisender Service** or the **www.Roisender.com** website for the performance of the **Service** by you or any third party. This **DPA** forms a supplemental, integral and indispensable part of the **Agreement** and your use of the **Roisender Service** and the **www.Roisender.com** website, whereby this **DPA** is subject to the provisions of Article 28 of the **GDPR.**
Consent shall mean any freely given, specific, informed and unambiguous indication of the **Data subject**'s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of **Personal Data** relating to him or her, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**.
Controller shall mean natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of **Personal Data**, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**. Please note, that even in the event that you are not in fact the **Controller** of **Personal Data** that you are using or wish to use in connection with the **Service**, you expressly warrant and represent to the **Provider,** that you have the necessary legal grounds and have obtained the required consent for the processing of the **Data subjects Personal Data** in connection with your use of the **Service** from the actual **Controller** of said **Personal Data**. In the context of this **DPA**, **Controller** shall mean you, the **User**.
Controller Personal Data shall mean any **End User Personal Data** or any other **Personal Data**, that the **Provider** or **Subprocessor Processes** or shall **Process** pursuant to or in connection with the **Agreement**.
Data processing (also **Processing**) means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In the context of this **DPA**, the **Provider** shall **Process** the **End User Data** for which the **User** is deemed as the **Controller** in order to provide the **Service**.
End User shall mean a natural or legal person with whom you, your **User Affiliates** or agents interact with through the **Roisender Service** or the **www.Roisender.com** website.**End User Messages** shall mean the **SMS Messages** that you send to the **End User** through the **Roisender Service** or the **www.Roisender.com** website as A2P "Application-to-person" messages.
European Economic Area (also called **EEA**) shall mean the EU Member States and Iceland, Liechtenstein, and Norway.
Including and similar words do not imply any limit.
Provider (also **we**, **us**, **our** or **Processor**) shall mean KOMPETENTNOST d.o.o., Žolgarjeva ulica 20, SI-2000 Maribor, Slovenia, EU, Company Registration Number: 6394329000, VAT ID Number: SI 83297286, the owner and supplier of the **Roisender Service** and the **www.Roisender.com** website who can be reached or through

the messaging application on the aforementioned website. In the context of this **DPA**, the **Provider** shall be deemed as the **Processor** of **Personal Data**.
Provider Affiliate shall mean shall mean in respect of the **Provider** and its legal entity, any other legal entity or private person controlling the **Provider** or being controlled by the **Provider**, or acting under the direct influence or instructions of the **Provider**, whereby "being controlled by" shall mean the possession, directly or indirectly, solely or jointly with another person, of power to direct or cause the direction of the management or policies and cations of a legal or natural person (whether through the ownership of securities, other shareholders, partnership or ownership interest, by establishing total or partial identity of individuals in management, by contract or otherwise).
Personal Data shall mean any information relating to an identified or identifiable natural person (herein after: **Data subject**), whereby an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**.
Personal Data Breach shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**.
Processor shall mean a natural or legal person, public authority, agency or other body which processes **Personal Data** on behalf of the **Controller**, as provided for by Article 4 of the **GDPR** or by any other relevant **Applicable legislation**. In the context of this **DPA**, the **Provider** shall be deemed as the **Processor** of **Personal Data**.
Party shall mean either you or the **Provider** whereby the term also includes that **Party**'s permitted assigns. The term Parties shall mean both you and the **Provider**.
Privacy policy shall mean the information to be provided to the **Data subject** where **Personal Data** are collected from the **Data subject**, as provided for by Article 13 of the **GDPR** or by any other relevant **Applicable legislation**.
Person includes an individual, a body corporate, an association of persons (whether corporate or not), a trust, a government department, or any other entity.
Personnel includes officers, employees, contractors, **User Affiliates** and agents of the **User.**
SMS Message shall mean a text message as defined in GSM 3GPP TS 23.038 standard (originally GSM recommendation 03.38). In the context of the **Service**, the message shall mean an A2P "Application-to-person" message.
Start Date shall mean the date that you set up an account/first use the **Roisender Service**.
Subprocessor (or **Contracted Subprocessor**) shall mean any person (including any third party and any **Provider Affiliate**, but excluding an employee of the **Provider** or any of its subcontractors) appointed by or on behalf of the **Provider** or any **Provider Affiliate** to **Process Personal Data** on behalf of the **Provider** in connection with the **Agreement.**
Standard contractual clauses shall mean the standard data protection clauses for the transfer of **Personal Data** to **Processors** established in countries outside of the **EEA**, where an adequate level of data protection with regards to the **GDPR** is not ensured on a national and systemic level, as described in Article 46 of the **GDPR**.
You (also **your**, **User**, **Controller**) shall mean the legal entity that shall be identified as the registered user of the **Service** when you, the duly authorised individual representing said entity, register an account (i.e. perform the actions from point 1.1. in the name the company you represent) is bound to this **Agreement** and the **Roisender Data Processing Agreement** in accordance with the terms herein. The aforementioned also relates to any and all **Permitted Users**, **Personnel**, or your **User Affiliates.** In the context of this **DPA** you shall be deemed as the **Processor** of **Personal Data**.
User Affiliate shall mean in respect of the **User** and his legal entity, any other legal entity or private person controlling the **User** or being controlled by the **User**, or acting under the direct influence or instructions of the **User**, whereby "being controlled by" shall mean the possession, directly or indirectly, solely or jointly with another person, of power to direct or cause the direction of the management or policies and cations of a legal or natural person (whether through the ownership of securities, other shareholders, partnership or ownership interest, by establishing total or partial identity of individuals in management, by contract or otherwise).
3.2. Words in the singular include the plural and vice versa.

3.3. A reference to the **Applicable legislation** or statute includes references to regulations, orders or notices made under or in connection with such legislation, statute or regulations and all amendments, replacements or other changes to any of them.

4. CONTRACTUAL INTENT AND TERM

4.1. The Parties seek to implement this **DPA** in order to achieve compliance with the requirements with the **Applicable legislation** as it pertains to the **Processing** of **Persona Data** and especially Article 28 of the **GDPR**, which forms the basis under which this **DPA** is drafted and construed.

4.2. Notwithstanding any other provision relating to the term of this **DPA**, this **DPA** will take effect on the **Star Date** and shall remain in force until the **Provider** has deleted or returned all **End User Personal Data** to the **Controller**, whereby it shall be deemed as automatically terminated.

5. PROCESSING OF CONTROLLER PERSONAL DATA

5.1 Permitted scope of Processing.

The **Provider** shall:

- **Process Controller Personal Data** in order to provide the **Service** as stated in the **Agreement** or on the basis of relevant **Controller**'s documented instructions which shall be deemed as contained herein unless otherwise given to the **Provider** in writing,
- comply with any and all **Applicable legislation** in the **Processing** of **Controller Personal Data,**
- **Process Controller Personal Data** if **Processing** is required under the **Applicable legislation** to which the **Provider** or relevant **Contracted Processor** is subject, in which case the **Provider** shall, to the extent permitted under the **Applicable legislation**, inform the **Controller** of that legal requirement before the relevant **Processing** of such **Personal Data** takes place.

5.2. For the avoidance of doubt, the **Provider** shall only use the **Controller Personal Data** to provide the **Service** and shall not keep, retain, disclose, make available to third parties, sell or otherwise use the **Controller Personal Data** for any purpose other than for providing the **Service** under the **Agreement** as further described in **Annex 1**.

5.3. The **Controller** instructs the **Provider** and each **Provider Affiliate** (and authorises the **Provider** and each **Provider Affiliate** to instruct each **Subprocessor**) to:

- **Process Controller Personal Data** as necessary for the provision of the **Service** as specified in **Annex 1**,
- transfer **Controller Personal Data** to any country or territory as reasonably necessary for the provision of the **Services** and consistent with the **Agreement** if such territory is in the **EEA**, as specified in sections 8 and 14.

5.4. The **Controller** warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 5.3. for all **Controller Personal Data** and on behalf of each relevant **Controller Affiliate**.

5.5. **Annex 1**to this **DPA** sets out certain information regarding the **Contracted Processors' Processing** of the **Controller Personal Data** as required by Article 28 of the **GDPR** (and, possibly, equivalent requirements of other Applicable Legislation). The **Controller** may make reasonable amendments to **Annex 1** by written notice to **Provider** from time to time as **Controller** reasonably considers necessary to meet those requirements. Nothing in **Annex 1** (including as amended pursuant to this section 4) confers any right or imposes any obligation on any party to this **DPA**.

6. Provider and Provider Affiliate Personnel

6.1. The **Provider** and each **Provider Affiliate** shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any **Contracted Processor** who may have access to the **Controller Personal Data**, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant **Controller Personal Data**, as strictly necessary for the purposes of the **Agreement**, and to comply with **Applicable legislation** in the context of that individual's duties to the **Contracted Processor**, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

7. Security and the keeping of records

7.1. Taking into account the state of the art, the costs of implementation and 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 **Provider** and each **Provider Affiliate** shall in relation to **the Controller Personal Data** implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32 of the **GDPR**.

7.2. The list of technical and organizational measures that the **Provider** and each **Provider Affiliate** offers the Controller under this **DPA** is included in **Annex 2**.

7.3. Prior to concluding the **Agreement** and this **DPA**, the **Controller** is required to review and analyse the contents of **Annex 2** with regards to the technical and organizational measures and other **security** commitments which the **Provider** offers in connection with the provision of the Service.
7.4. In assessing the appropriate level of security, the **Provider** and each **Provider Affiliate** shall take into account the particular risks that are presented by **Processing Personal Data** and in particular the risk of a **Personal Data Breach**. The **Controller** understands and agrees, that it is his sole responsibility to consider if the technical and organizational measures from **Annex 2** meet his security needs and obligations with regards to **Controller Personal Data** and the **Applicable legislation**.
7.5. Regarding the aforementioned, the **Controller** understands and agrees, that he is solely responsible for his use of the **Service**, and is asked to put in place and maintain his own technical and organizational measures, which must include industry-level best practices such as:

- making copies (i.e. backing up) all **Controller Personal Data** prior to use with the **Service**,
- practicing safe and secure usage of the Service and the user account/password (secure keeping of account authentication credentials,
- securing systems and devices which are used to access or interact with the Service.

7.6. The **Provider** and **Provider Affiliate** take no responsibility regarding the processing, storage and protection of **Controller Personal Data** outside of the **Service** and the subsystems connected to the **Service** (which includes but is not limited to the access and storage of **Controller Personal Data** on the servers of the Controller or a third party, the transferring of **Controller Personal Data** to third parties, the distribution of account authentication credentials to third parties, etc.).
7.7. The **Controller** understands and agrees that by concluding the **Agreement** and this **DPA**, the technical and organizational measures from **Annex 2** as well as other aspects of the security are deemed as appropriate with regards to the risk posed to **Data Subjects**.
7.8. To the best of his ability the **Provider** shall keep records (i.e. log files) regarding the **Processing of Controller Personal Data**, and shall ensure that the records are sufficient to meet the **Controllers** compliance requirements. The **Provider** shall also provide said records to the **Controller** upon his written request.
8. Subprocessing
8.1. The **Controller** specifically authorizes and generally agrees with the **Provider** and each **Provider Affiliate** appointing and engaging **Subprocessors** in accordance with this section 8 and any restrictions in the **Agreement**.
8.2. The **Provider** and each **Provider Affiliate** may also continue to use those **Subprocessors** already engaged by the **Provider** or any **Provider Affiliate** at the Start Date, whereby the **Provider** and **Provider Affiliate** shall be in each case and as soon as practicable required to ensure that the obligations set out in this section 8. are met by such **Subprocessors**.
8.3. The list of **Subprocessor**, including details regarding their location and **Processing** functions is available here and may be updated from time to time by the **Provider**.
8.4. Regarding the **Processing and subprocessing of Controller Personal Data**, the **Provider** and any **Provider Affiliate** shall only appoint and engage **Subprocessor** through the conclusion of a data processing agreement containing all necessary data protection obligations, which shall offer the same level of data processing protection that can be found in this **DPA**, to the extent applicable to the nature of the **Services** provided by such **Subprocessors**.
8.5. **Ten (10) business days prior** to any **Processing** being carried out by a newly appointed **Subprocessor**, the **Provider** shall add such newly engaged **Subprocessor** to the list of **Subprocessors**. The parties hereby agree that such method of notification is adequate with regards to the **Controllers** right to be notified prior to **Subprocessor engagement**.
8.6. Should the **Controller** or **Controller Affiliate** oppose the engagement and appointment of a new **Subprocessor**, he shall notify the **Provider** within **ten (10) business days** from the last day prior to the start of **Processing** as referred to in the previous point. After that, **Processing** by the **Subprocessor** shall be deemed as accepted by th**e Controller** or **Controller Affiliate**.
8.7. Should the **Controller** or **Controller Affiliate** oppose the engagement and appointment of a new **Subprocessor** and notify the **Provider** regarding this (even after the period from the previous point), all data processing by such newly appointed Subprocessor shall cease and the parties shall seek to find an applicable solution in good faith. If the parties cannot agree on an applicable solution regarding the objection in a reasonable timeframe, the Controller may terminate the Agreement.
8.8. The **Provider** may be held liable for all obligations subcontracted to the **Subprocessors**, including their acts and omissions.
9. Data Subject Rights

9.1. Taking into account the nature of the **Processing**, the **Provider** and each **Provider Affiliate** shall assist the **Controller** by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controllers' obligations to respond to requests to exercise **Data Subject** rights under the **GDPR** and the **Applicable legislation**.

9.2. The **Provider** shall:

- promptly notify the **Controller** if any **Contracted Processor** receives a request from a **Data Subject** under the **GDPR** and the **Applicable legislation** in respect of **Controller Personal Data**; and
- ensure that the **Contracted Processor** does not respond to that request except on the documented instructions of the **Controller** or the relevant **Controller Affiliate** or as required under the **GDPR** and the **Applicable legislation** to which the **Contracted Processor** is subject, in which case the **Provider** shall to the extent permitted by **Applicable legislation** inform the **Controller** of that legal requirement before the **Contracted Processor** responds to the request.

10. Personal Data Breach

10.1. The **Provider** shall notify the **Controller** without undue delay upon the **Provider** or any **Subprocessor** becoming aware of a **Personal Data Breach** affecting the **Controller Personal Data**, providing the **Controller** with sufficient information to allowing him to meet any obligations to report or inform the **Data Subjects** of the **Personal Data Breach** under the **Applicable legislation**.

10.2. The **Provider** shall co-operate with the **Controller** and take such reasonable commercial steps as are directed by the **Controller** to assist in the investigation, mitigation and remediation of each such **Personal Data Breach**.

11. Data Protection Impact Assessment and Prior Consultation

11.1. The **Provider** and each **Provider Affiliate** shall provide reasonable assistance to the **Controller** with any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, which the **Controller** reasonably considers to be required under Article 35 or 36 of the GDPR or equivalent provisions of any other **Applicable legislation**, in each case solely in relation to the **Processing of Controller Personal Data** by, and taking into account the nature of the **Processing and information** available to, the **Provider** and the **Contracted Processors**.

12. Deletion or return of Controller Personal Data

12.1. Subject to points 12.2 and 12.3 the **Provider** and each **Provider Affiliate** shall promptly and in any event **within 15 (fifteen) business days** of the date of termination of the **Agreement** (i.e. termination by either the **Controller** or the **Provider** under the applicable clauses of the Agreement) delete and procure the deletion of all copies of those Controller Personal Data, that are listed as being stored in Annex 1, thereby permanently removing all copies and instances of such data in the **Provider's systems**. By notifying the **Provider** prior to termination of the Agreement, the **Controller** and **Provider** may also arrange for the transfer of such data to the **Controller** prior to deletion.

12.2. The **Provider** and each **Contracted Processor** may retain **Controller Personal Data** to the extent required by **Applicable legislation** and only to the extent and for such period as required by the **Applicable legislation** and always provided that the **Provider** and each **Provider Affiliate** shall ensure the confidentiality of all such **Controller Personal Data** and shall ensure that such **Controller Personal Data** is only **Processed** as necessary for the purpose(s) specified in the **Applicable legislation** requiring its storage and for no other purpose.

13. Audit rights

13.1. Subject to sections 13.2 to 13.4, the **Provider** and each **Provider Affiliate** shall make available to the **Controller** on request all information necessary to demonstrate compliance with this **DPA**, and shall allow for and contribute to audits, including inspections by the **Controller** or an auditor mandated by the **Controller** in relation to the **Processing of the Controller Personal Data** by the **Controller** or the **Contracted Processors**.

13.2. Information and audit rights of the **Controller** only arise under section 13.1 to the extent that the **Agreement** does not otherwise give information and audit rights meeting the relevant requirements of the **Applicable legislation** (including Article 28 of the GDPR).

13.3. The **Controller** or the relevant **Controller Affiliate** undertaking an audit shall give the **Provider** or the relevant **Provider Affiliate** a notice at least **fourteen (14) business day prior** to any audit or inspection being conducted under this section 13 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the **Providers** or **Contracted Processors**' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. The **Provider** or a **Contracted Processor** need not give access to its premises for the purposes of such an audit or inspection

- to any individual unless he or she produces reasonable evidence of identity and authority;
- outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the **Controller** or the relevant **Controller Affiliate** undertaking an audit has given notice to the **Provider** or the relevant **Provider Affiliate** that this is the case before attendance outside those hours begins; or
- for the purposes of more than one audit or inspection, in respect of the **Provider** or each **Contracted Processor**, in any calendar year, except for any additional audits or inspections which:
    . the **Controller** or the relevant **Controller Affiliate** undertaking an audit reasonably considers necessary because of genuine concerns as to **Provider's** or the relevant **Provider Affiliate's** compliance with this **DPA**; or
    a. the **Controller** is required or requested to carry out by the **Applicable legislation**, a supervisory authority or any similar regulatory authority responsible for the enforcement of **Applicable legislation** in any country or territory.

13.4. The Provider shall, upon request also provide the Controller or the mandated auditor with documentation of implemented technical and organizational measures to ensure an appropriate level of security, and other information necessary to demonstrate the Provider's or the relevant Provider Affiliate's or the Contracted Processor's compliance with its obligations under this DPA and relevant Applicable legislation, but shall provide access to information concerning the Provider's or the relevant Provider Affiliate's or the Contracted Processor's other information subject to confidentiality obligations.

14. Transfer of Controller Personal Data to Countries Outside of the EEA

14.1. Transfer of **Controller Personal Data** to countries located outside of the **EEA**, hereunder by transfer, disclosure or provision of access to data, may only occur in case of documented instructions from the **Controller** or **Controller Affiliate**.

14.2. By entering into this **DPA**, the **Controller** also grants the **Provider** the authority to enter into **Standard contractual clauses** on behalf of the **Controller** or the relevant **Controller Affiilate**, as they may be laid down by the European Commission or the applicable supervisory authority from time to time, in order to secure a valid legal basis for the transfer, disclosure or provision of access to data by **Subprocessors** outside of the EEA or international organisations, whereby any such **Subprocessors** shall be approved in accordance with the procedure stipulated in section 8. od this **DPA**. If the **Controller** is not the actual controller of the relevant **Controller Personal Data**, the **Controller** shall ensure such authorisation from the actual controller. Upon request, the **Provider** shall provide the **Controller** with a copy of such **Standard contractual clauses** or state such other valid legal basis for each transfer.

14.3. The **Controller** accepts and understands that the transfer of **Controller Personal Data** to **Subprocessors** who are telecommunications operators in countries outside of the **EEA** might be necessary in order to transmit messages to recipients located in such countries, whereby the **Controller** agrees that entering into **Standard contractual clauses** prior to any **Processing of Controller Personal Data** by the **Provider** in such situations might be necessary, whereby the **Controller** shall notify the **Provider** regarding this prior to his use of the **Service**.

15. General Terms

15.1 Governing law and jurisdiction.

Without prejudice to any applicable **Standard contractual clauses** which may have been entered into on the basis of this **DPA**:

- with respect to any disputes or claims howsoever arising under this **DPA**, including disputes regarding its existence, validity or termination or the consequences of its nullity, the parties to this **DPA** hereby agree to submit to the laws of the Republic of Slovenia, whereby the **Controller** or **Controller Affiliate** consents to the exclusive jurisdiction of the courts located in the Republic of Slovenia whereby the place of venue shall be Ljubljana, Slovenia; and
- whereby the aforementioned laws, courts and venues shall be used regarding all non-contractual or other obligations arising out of or in connection with this **DPA**.

15.2. Order of precedence.

With regard to the subject matter of this **DPA** and in the event of inconsistencies between the provisions of this **DPA** and any other agreements between the parties, including the **Agreement** and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this **DPA**, the provisions of this **DPA** shall prevail.

15.3. Liability.

Under or in connection with the **Agreement**, this **DPA** or any **Standard contractual clauses** which may have been concluded in connection with this **DPA** and regardless of the type of liability, the parties hereby agree,

that the total combined liability of the **Provider** and the **Provider Affiliate** towards the **Controller**, the **Controller Affiliate** or towards both, shall be limited to limitations on liability or other liability caps agreed to by the parties in the **Agreement**.
The aforementioned shall not affect each parties liability to **Data subjects** under the **GDPR** or **Applicable legislation** or any **Standard contractual clauses** which may have been concluded in connection with this **DPA** to that such limitation of liability or liability cap would directly breach the GDPR or the **Applicable legislation**.

15.4. Severance

Should any provision of this **DPA** be invalid or unenforceable, then the remainder of this **DPA** shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

ANNEX 1: DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Controller Personal Data as required by Article 28(3) of the **GDPR**:

Method and purpouse of data collection

In order to provide the **Service** as it is set out in the **Agreement:**

a. the **Controller** may use the **Service** together with the input fields on his check-out page, whereby **Controller Personal Data** is entered into the **Service** by the **End Users** themselves;
b. the **Controller** may input **Controller Personal Data** directly into the **Service** himself;

In both cases outlined above, the **Provider** is therefore instructed by the **Controller** under this **DPA** to collect, store and process the relevant data, so that the **Controller** may send **SMS messages** to his relevant and consenting **End Users**.

Categories of Data Subjects

The categories of **Data Subjects** whose **Personal data** may be **Processed** under this **DPA** are defined by the **Controller** and are as follows:

- **Controller's End Users** (i.e. subjects who enter their mobile phone number and other information into the **Controller's** relevant check-out input fields, so that they may receive **SMS Messages** from the **Controller**);
- other **Data Subjects** (i.e. when the **Controller** enters and uses data of any other **Data Subjects** in connection with the **Service**);

whereby the **Controller** expressly warrants to the **Provider** under the **Agreement**, that he obtained the required consent for the processing of the **Personal Data** of any and all **Data Subjects**.

Personal Data types and the subject-matter, nature and purpose of Processing

Subject to the **Controller's** use of the **Service**, the following **Processing** may be carried out by the **Provider** or his **Subprocessors** in order to provide each sought after feature of the **Service**:

Personal Data Type* / Other information	**Subject-matter and nature of processing**	**Purpose of processing**
Event / User Action type *(purchase completion, cart abandonment, newsletter subscription)*	Automatically collecting, segmenting and storing each **End User** event / action relating to purchase completion, cart abandonment or newsletter subscription.	So that **Controllers** may better segment the **End Users** based on their events or the actions that they performed on their website (completion of the purchase, subscription to the newsletter, the abandonment of their cart). This type of segmentation allows Controllers to customize / select / draw-up the appropriate contents of their **End User Messages**.
	Automatically collecting and storing website / storefront type data.	Different platforms work in different ways (implementation of discounts and discount codes, different ways of

		generating URLs at the end of the check-out process and different ways of restoring the contents of an abandoned cart). In order to properly process the data and send a compatible link, discount code, coupon code, etc. with regards to the website / storefront and for the **Service** to be compatible with different platforms, data on the platform sending the API call is required.
Service widget/plug-in version data	Automatically collecting and storing **Service** widget/plug-in version data.	To reduce the possibility of errors and incompatibilities with older versions of our widget/plug-in, we collect data about the version in use by the **End User**.
Basic End User Contact Information (*Phone Number, delivery address, IP address, Name, Surname*)	Automatically collecting, storing and using such data when the **Customer** wishes to send **End User Messages.**	So that the Controller may send **End User Messages** to such **Data Subjects**. To recognise and use the relevant phone number prefix based on the **End User's** country prefix number. So that prepopulated **End User Messages** and **End User Message** templates may be personalised by the **Controller** with the **End User's** name, surname and further contextualised with regards to his delivery address. Collecting and processing the End User IP address falls under the category of legitimate interest of the **Provider**, whereby this data is processed in order to defend the **Service** from DDOS attacks.
Data relating to the End User's Cart *(Cart value, Chosen currency, Chosen Payment Method, Coupon code, URL to complete the purchase Cart Contents -Product ID, Product Name, Quantity, Product Price)*	Automatically collecting, storing and using such data for when the **Controller** wishes to send **End User Messages.**	So that the **Controller** may offer **End Users** a way to restore the contents of their previously abandoned cart. Used for the personalization of **End User Messages** and for the conditional logic of sending such messages. So that the **Controller** may offer valid discount coupons to his **End Users.** Each check-out page has a different URL and thereby storing the relevant URL of a particular abandoned cart is essential

		for restoring the contents of a previously abandoned cart.
Values of checkboxes *(Cart Abandonment SMS consent, Marketing SMS consent, Newsletter consent)*	Automatically collecting and storing data on whether the checkbox is displayed, what content it relates to and whether the **End User** has checked it.	This data is processed in order to collect and store evidence regarding **End User** consent, so that the Controller can legally send **End User Messages** via the **Service**. Similarly, processing and storing this data stems from our legitimate interest to provide information on why an **End User** received a **End User Message**.
Traffic data	Automatically collecting and storing technical as well as **Personal Data** in relation to the conveyance of communications on an electronic communications network or billing thereof.	This data is processed in order for the communication with the **End User** to take place (i.e. in order for the SMS Message to be sent) and for the appropriate charge to be paid to the communications provider and includes information about the routing and timing of the **SMS Message**.
End User Message content data *(i.e. the actual contents/text of the SMS Message)*	Automatically collecting and storing technical as well as **Personal Data** in relation to the conveyance of communications on an electronic communications network.	This data is processed in order to provide the key feature of the **Service** (i.e. to allow the **Controller** to communicate with **End Users** via **End User Messages**).

Special categories of Personal Data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or health data, may be processed under this **DPA if the Service are used by the **Controller** to process such data.*

Timescales for the keeping of Personal Data and the duration of the Processing

The **Provider** will keep **Personal Data** for as long as it is necessary to fulfil the purposes for processing and shall delete and procure the deletion of all copies of stored **Personal Data** within within 15 (fifteen) business days of the date of termination of the **Agreement** (i.e. termination by either the **Controller** or the **Provider** under the applicable clauses of the **Agreement**).

The processing will continue for the duration of **Controller**'s use of the **Service**, whereby most **Processing** takes place instantly after initiation by the **Controller** via the **User** dash board.

Entities involved in the Processing

Personal Data shall firstly be processed by the **Controller** when entering the data into the **Service**. The data will further be processed in order for messages to be set up as required by the **Controller**, and the list of recipients to be correct, before the process for sending the defined **End User Messages** to the defined recipients is initiated.

Secondly the **Personal Data** shall mainly be processed via automatic means by the **Service** algorithms and software systems (i.e. automatic storage of applicable data, processing of recipients telephone numbers prior to transmission of **End User Messages**, etc.). **Provider Personnel** shall only process **Personal Data** upon **Controller** request or when performing job related tasks that require the **Processing** of data (i.e. the upkeep and monitoring of system and functions, troubleshooting, etc.).

Approved Subprocessors

The following **Subprocessors** are hereby jointly approved by the **Controller** in relation to the provision of the **Service** under this **DPA**.

In accordance with this **DPA**, the **Provider** is instructed by the Controller to transfer **Personal Data** to the listed **Subprocessors**:

Subprocessor	Type of processing	Country, location
Atman S.A, ul. Grochowska 21 a, 04-186	Hosting / SMSAPI (customer panel, API	Polan
Google Ireland Limited	Storage of data on the Google Cloud service.	Frankfurt – Germany – EU
T-Mobile Polska S.A, ul. Marynarska 12, 02-	Hosting / SMSAPI (customer panel, API	Poland

ANNEX 2: LIST OF TECHNICAL AND ORGANIZATIONAL MEASURES OFFERED BY THE PROVIDER AND PROVIDER AFFILIATE

1. PHYSICAL ACCESS CONTROL

The entrance to the common areas and the office is under supervision, with the key to the entrance of the office being held only by the head of the office, the director and any other supervising employees.
Cabinets, desks and other office furniture in which personal data carriers are kept and which are located outside the protected areas (corridors, common areas) are locked. The keys are kept by the employee who supervises the individual cabinet or desk at a designated place. Leaving keys in their locks is not allowed.
Access to the protected premises is allowed only during regular working hours, whereby access at a different time is only allowed with the permission of the responsible person (supervising employee).
Cabinets and desks containing personal data carries are locked in protected rooms at the end of working hours or after the completion of work after working hours, while computers and other hardware are switched off and physically locked or locked through software. Leaving keys in their locks is not allowed.
Employees ensure that persons who are not employees of the company (e.g. customers, maintenance staff, business partners, etc.) do not enter the protected premises unattended, but only with the knowledge / presence of the responsible person.

2. PROTECTION OF DATA CARRIERS CONTAINING PERSONAL DATA DURING WORKING HOURS

Personal data carriers are not left in visible places (e.g. on desks) in the presence of persons who do not have the right to inspect them.
Data carriers containing sensitive or special types of personal data shall not be stored outside secure premises.
Data carriers containing personal data may be removed from the premises of the company only with the permission of the supervising employee, whereby the supervising employee shall be deemed to have given permission by engaging a certain associate in a task which includes the processing of personal data outside the protected premises.
In the premises, which are intended for performing business with external collaborators and others, data carriers which contain personal data and computer displays are placed in such a way that, external collaborators do not have access to them.

3. HARDWARE AND SOFTWARE PROTECTION

SSL encryption and “SALT” hash encryption.
Maintenance and repair of hardware, computer and other equipment is allowed only with the knowledge of the responsible person, and it is performed only by authorized services and maintenance personnel who have concluded appropriate contracts with the company.
Access to the software is protected by allowing only employees designated by the supervising employee, including legal or natural persons who, in accordance with the contract, provide the agreed services.
Workers may not install software without the knowledge of the supervising employee. They may also not uninstall software owned by the company, delete, or copy its data or transfer it to another medium/carrier/processor/controller without the consent of the supervising employee.

<u>3.1. Accessing data via application software and changing passwords</u>

Access to data via application software is protected by a system of passwords for authorization and identification of users of programs and data whereby 2FA is used.