Appendix no. 1 to the Order Form - Terms and conditions

§1 General provisions

1. SALESmanago and the Customer unanimously confirm that they are bound by an agreement to licence the SALESmanago System - "**System**" ("**Licence Agreement**").
2. Based on the Order Form and these Terms and Conditions, SALESmanago and the Customer enter into an agreement based on which SALESmanago provides the Customer with SMS messaging services (the "Services"), including the package selected by the Customer (the "Agreement").

§2 General terms and conditions of service

1. The Services are provided with the participation of Vercom S.A., based in Poznań (60- 829), at: 22 Franklin Roosevelt Street, entered in the Register of Entrepreneurs of the National Court Register kept by the District Court Poznań - Nowe Miasto and Wilda in Poznań, VIII Economic Department of the National Court Register under KRS number: 0000535618, NIP: 7811765125, REGON: 300061423 ("Vercom"). SALESmanago may, for valid reasons, change the service provider from Vercom to another entity, to which the Customer agrees.
2. SALESmanago will agree with the Customer on planned maintenance breaks via email, at least 24 hours in advance. The information will include the start time of the interruption and the approximate end time.
3. SALESmanago may, for valid reasons, temporarily interrupt or substantially limit the provision of the Services or change the terms and conditions of their provision if there are legitimate circumstances that make it impossible to meet the requirements for maintaining the continuity of the provision of the Services, independent of SALESmanago, such as, in particular, failure of the telecommunications network, natural disasters, situations of special emergency and the need to protect the integrity of the network.
4. SALESmanago is not responsible for messages (and their content) sent at the request of the Customer or by the Customer as part of the Services provided to the Customer. In addition, SALESmanago is not responsible for: (i) messages sent late, (ii) messages that could not be sent due to technical reasons beyond SALESmanago's control (e.g. GSM operator failure, natural disasters, etc.), (iii) messages that could not be sent due to exceeding the limit applicable under the package selected by the Customer.
5. Ordering by the Customer to send SMS messages is possible only to standard telephone numbers operated by Polish or foreign mobile operators. This means that, in particular, it is not possible for the Customer to order the sending of SMS messages to premium rate telephone numbers or to landline telephone numbers. However, ordering dispatch to telephone numbers operated by foreign operators is only possible if this is specified in the price list.
6. The Customer may order for sending an SMS message containing up to 918 characters from the GSM 7bit alphabet, and for the purpose of calculating SALESmanago's remuneration, the SMS message fee indicated in the price list will be calculated per 160 characters from the GSM 7bit alphabet in the case of a single SMS message, and per each started 153 characters from the GSM 7bit alphabet if the SMS message contains more than 160 characters from the GSM 7bit alphabet.
7. If the Customer orders an SMS message to be sent that contains characters other than characters from the GSM 7bit alphabet, in particular Polish diacritics ("Polish font"), the maximum length of the SMS message is 402 characters, whereby for the purpose of calculating SALESmanago's remuneration, the SMS message fee indicated in the price list will be calculated per 70 characters for a single SMS message, and per each started 67 characters if the SMS message contains more than 70 characters.

8. The Customer is obliged to duly secure access to the account in the System against unauthorised access. The Customer is responsible (including the obligation to pay remuneration) for all SMS sending orders made from the account in the System.

§3 Prohibited activities

1. Throughout the term of the Agreement, the Customer agrees to: (i) refrain from providing content that is contrary to the law or good morals, including the rules of social coexistence, that violates or threatens the rights, including the personal rights of third parties and entities, that violates intellectual property rights, that calls for racial, ethnic, religious, cultural hatred and concerning sexual orientation, that promotes pornography or violence - in any form, and (ii) refrain from sending commercial information within the meaning of the Polish Act of July 18, 2002 on the provision of electronic services without the prior consent of the addressee.
2. It is prohibited to use the Services to send communications containing unlawful content, as well as to use telecommunications terminal equipment and/or automatic calling systems for direct marketing purposes without the prior consent of the addressee. It is the Customer's responsibility to collect all legally required consents from recipients of directed communications.
3. Before using the Services, the Customer shall read Vercom's Anti-spam Policy, the current version of which, as at the date of conclusion of the Agreement, is attached to the Order Form and the current version of which is available here ("Anti-spam Policy"). Throughout the term of the Agreement, Customer shall comply with the provisions of the Anti-spam Policy, and any action contrary to the Anti-spam Policy shall constitute a grave breach of the Agreement and may result in SALESmanago terminating the Agreement without notice or, at SALESmanago's option, suspending the Service until the matter is clarified (with SALESmanago retaining the right to receive compensation for the period of suspension of the Service). The Anti-spam Policy is an integral part of the Agreement. The Anti-spam Policy may be subject to change, which the Customer is obliged to monitor. A change in the Anti-spam Policy does not require an annex to the Agreement. For the purposes of this Agreement, "Client" for purposes of the Anti-spam Policy will be deemed to be Customer, where applicable, and "Vercom" for purposes of the Anti-spam Policy will be deemed to be SALESmanago, where applicable.
4. Violation by the Customer or the Customer's client of the provisions of paragraphs 1-3 above constitutes a gross violation of the Agreement and entitles SALESmanago to terminate the Agreement with immediate effect. The provisions of paragraph §7.2 of the Terms and Conditions shall apply accordingly.

§4 Fees and payments

1. The Customer shall pay the fees due to SALESmanago for the provision of the Services.
2. The credits purchased by the customer can be used to send SMS messages. The cost of sending (the number of credits needed) SMS messages varies, depending on the location of the recipient of the message and its length. The price list for sending SMS messages may change over time. SALESmanago does not guarantee the invariability of prices for sending SMS messages. The System allows the Customer to make a non-binding estimate of the cost of a specific SMS dispatch by the Customer. The final cost of a specific SMS message dispatch is known after the dispatch.
3. In the event that the current number of credits does not allow for the execution of the Customer's scheduled mass message dispatch, the Customer will be informed of this in an appropriate message in the System. After accepting the additional cost resulting from exceeding the number of credits within the package selected by the Customer, the Customer will be able to execute the scheduled mass message dispatch.

4. Automated dispatches resulting from automation processes will not require approval, even if the available amount of credits in the package is exceeded, to which the Customer agrees.
5. The payment terms for the Services are agreed in the Order Form. Failure to make timely payment may result in the initiation of bad debt collection proceedings, the imposition of interest for late payment or the temporary restriction of System functionality (and this restriction does not affect the remuneration payable to SALESmanago).
6. The commitment to pay for the selected package is irrevocable, and the fees paid are non-refundable.
7. All amounts due or payable by the Customer under this Agreement shall be paid free and clear of any deduction, withholding or set off.
8. The unused credit limit of the package selected by the Customer is not refundable or convertible into cash equivalent.

§5 Personal data protection

1. The Parties have regulated the principles of entrusting the processing of personal data in the provision of the Services in the Personal Data Processing Entrustment Agreement, which is attached to the Order Form.
2. To execute the Agreement, the Parties, as independent data controllers, will share the personal data of their representatives indicated in the Agreement, representatives and persons appointed to execute the Agreement, including the following categories of data: identification data (including, but not limited to, name, position of representative). In connection with the execution of the Agreement, the Parties may also transfer the personal data of employees and associates not listed in the Agreement.
3. SALESmanago implements the information obligation to representatives and employees whose data is listed in the Agreement through the information clause, attached as Appendix 3 to the Order Form.

§6 Liability

1. In no event shall the aggregate liability of SALESmanago arising out of or related to the Agreement exceed the total amount paid by Customer hereunder for the services giving rise to the liability in the twelve months preceding the first incident out of which the liability arose or € 10,000, whichever amount is lower.
2. In no event will SALESmanago have any liability arising out of or related to the Agreement for any lost profits, revenues, goodwill, or indirect, special, incidental, consequential, cover, business interruption or punitive damages. The foregoing disclaimer will not apply to the extent prohibited by law.

§7 Duration and termination of the Agreement

1. The Agreement is concluded for an indefinite period and may be terminated by either Party with 30 days' notice effective at the end of the three-month credit settlement period.
2. Expiration of the Licence Agreement shall result in expiration of the Agreement.
3. SALESmanago shall be entitled to terminate this Agreement immediately, i.e. without notice in any case of gross violation of the provisions of this Agreement by the Customer, in particular in case of: (i) violation of any of the provisions of §3 paragraphs 1-3 of the Terms and Conditions, or (ii) the Customer's failure to pay invoices in which the delay in payment exceeds 30 days.
4. In the event of termination of the Agreement, the fee paid for unused credits is not refundable.

§8 Miscellaneous

1. Neither Party will be liable for any delay or failure to perform its obligation under the Agreement if the delay or failure is due to extraordinary and unforeseeable event or circumstance beyond its reasonable control (force majeure), such as a strike, blockade, war, act of terrorism, riot, natural disaster, failure or reduction of power or telecommunications or data networks or services, or government act.
2. SALESmanago reserves the right to amend the provisions of the Agreement, as well as any other documents applicable to the Services provided hereunder, in the event of:
   2.1. expansion of the scope of the Services provided, introduction of new functionalities or options, improvement of the parameters of the Services, modernization of the technology or improvement of the process and/or the way the Services are organised on its basis, making the Services available to other categories of customers (e.g. consumers),
   2.2. change of law requiring changes to the Agreement and other documents applicable to the Services provided under it,
   2.3. issuance of court rulings or other binding rulings of public authorities affecting SALESmanago's operations or provision of the Services specified in the Agreement, in particular those concretizing or imposing new obligations on SALESmanago with respect to the provision of the Services,
   2.4. withdrawal from the offer of the Services, their elements, functionalities,
   2.5. increase in the cost of SALESmanago's business caused by an increase in the cost of labour (minimum wage, average monthly salary in the corporate sector), increase in prices (including an increase in the level of the annual inflation index published by the Central Statistical Office or the prices of goods or services of SALESmanago's contractors, increase in the cost of acquiring, performing, upgrading or maintaining the infrastructure necessary to provide the Services);
   2.6. the occurrence of an event of force majeure understood as a phenomenon of an extraordinary nature (having a military or natural cause or resulting from an action of public authority), which could not be prevented by ordinary means, and for which SALESmanago is not responsible, as a result of which it is not possible for SALESmanago to provide the Services in the existing scope or on the existing terms and conditions,
   2.7. the need, on the part of SALESmanago, to modify the Agreement by making stylistic or editorial changes, as well as those aimed at clarifying individual provisions of the Agreement, in a manner that does not interfere with the rights and obligations of the Parties, but is intended to promote clarity of the document,
   2.8. the need to adapt the provisions of the Agreement to the applicable legal regulations.
3. Subject to paragraph 4 below, SALESmanago will inform the Customer about the planned change in the provisions of the Agreement well in advance, in any case not less than 14 days before the planned changes take effect.
4. In particularly justified cases, the deadline for informing the Customer about the planned change to the provisions of the Agreement may be shortened if SALESmanago is unable to meet it for reasons beyond its control.
5. Subject to the provisions of the Terms and conditions stating that the Agreement may be amended, any amendment or variation to the Agreement must be in writing or a document form via the digital signature tools (e.g. DropboxSign). Otherwise null and void. The Parties exclude the application of Art. 66^1 § 1-3 of the Polish Civil Code.
6. If any provision of the Agreement is held by a court or other competent authority to be unlawful, void or unenforceable, it shall be deemed to be deleted from the Agreement. It shall be of no force and effect, and the Agreement shall remain in full force and effect as if such provision had

not originally been contained in the Agreement. In the event of any such deletion the Parties shall negotiate in good faith in order to agree the terms of a mutually acceptable and satisfactory alternative provision in place of the provision so deleted.

7. The Agreement is governed by and constructed under Polish law.
8. Any dispute in connection to the Agreement shall be subject to the exclusive jurisdiction of the courts having jurisdiction over SALESmanago registered office.
9. If a conflict occurs between this Order Form, Terms and conditions or the Licence Agreement, unless otherwise specifically stated in these documents, the order of precedence shall be:
   9.1. Order Form
   9.2. Terms and conditions
   9.3. Licence Agreement.

Appendix no. 2 to the Order Form - Personal Data Processing Agreement

Personal Data Processing Agreement

hereinafter referred to as „PDPA”

between
Customer, hereinafter referred to as “**Entruster**”
and
SALESmanago, hereinafter referred to as “**Processor**”

Whereas,
the Parties have concluded the Agreement, Parties hereby agree as follows:

§ 1 Statements of the Parties

1. The Entruster declares that, regarding the entrusted personal data, it is either the data controller or the processor and has the right to process the data and entrust its processing.
2. The Processor shall ensure that appropriate technical and organisational measures are implemented so that the processing meets the requirements of the Act and the GDPR and provides the protection of the rights of the data subject.
3. The Processor declares that he applies all required technical and organisational measures so that the processing is carried out in accordance with Article 32 of the GDPR.
4. The Processor declares that the Processor has the resources, including infrastructure resources, experience, knowledge, and qualified personnel, to the extent that it is able to duly perform the PDPA, in compliance with the applicable laws. In particular, the Processor declares that it is familiar with the principles of personal data processing and security resulting from the GDPR.

§ 2 Subject matter of PDPA

1. Parties agree that for the purpose of fulfilling statutory obligations imposed by law, these being, in particular, the provisions of GDPR and the provisions of other Member States data protection laws that apply to the Agreement as well as the proper performance of the Agreement, the Entruster, entrusts the Processor with the processing of personal data in the scope as defined by this PDPA.
2. The Parties declare that processing is to be carried out on behalf of the Entruster and the Processor provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.
3. Where terms defined in the GDPR are used in this PDPA, these terms have the same meaning as in the GDPR.

§ 3 Description and scope of processing

1. This PDPA applies to the processing of personal data set out below:
   a. categories of data subjects: clients and potential clients of the Entruster;
   b. the type of personal data: phone number, name and surname, other personal data which processing is necessary to conclude the Agreement, which do not belong to special categories of personal data;
   c. the nature and purpose of personal data processing: performing the Agreement, using resources provided by the Processor;
   d. the subject-matter of the processing: personal data stored in the System in the duration of the same term as the performance of the Agreement.
2. The Parties jointly agree that the Entruster entrusts the Processor only with personal data within the scope of and concerning the categories of persons specified in § 3(1) of the PDPA. In entrusting a broader scope of personal data than in § 3(1) of the PDPA (in particular special categories of personal data/sensitive data), the Entruster is obliged to indicate in the Order Form a new scope of personal data that will be entrusted on the date of the Agreement. If the scope of processed personal data changes during the execution of the Agreement, the Entruster is obliged to indicate a new scope of personal data to the Processor.
3. The Processor undertakes to process entrusted personal data only for the purpose and scope specified in above, based on documented instructions from the Entruster, which also applies to the transfer of personal data to a third country or international organisation (unless such obligation is imposed by Union law or the law

of the Member State to which the Processor is subject; in this case, the Processor shall inform the Entruster of this legal obligation prior to the commencement of processing, unless such law prohibits the provision of such information on grounds of important public interest).

§ 4 Rights and obligations of Parties

1. The Entruster entrusts the Processor with the personal data collected and processed only in accordance with the law, and when the law requires obtaining the consent of the data subject for the processing of personal data or consent to which the data protection laws apply, the Entruster undertakes to obtain the said consents, in the manner prescribed by such laws.
2. Following a written request by the Entruster, the Processor shall, to the extent possible and reasonable, be obliged to provide information regarding the processing of personal data entrusted to him, including details of technical and organisational means used for the purpose of processing data. The request mentioned above may be made only when the Entruster has not been able, after making its best efforts, to obtain information regarding the processing of the entrusted personal data on its own (e.g., by verifying documents and correspondence previously sent by the Processor).
3. The Processor shall inform the Entruster prior to the commencement of processing of data on the implementation of a possible legal obligation consisting of the transfer of personal data to a third country or an international organisation, in accordance with Article 28(3) point a of the GDPR.
4. The Processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, in accordance with Article 28(3) point b of the GDPR.
5. The Processor undertakes to ensure that every person acting under the authority of the Processor who has access to personal data processes them only at the request of the Entruster for the purposes and scope provided for in the PDPA.
6. The Processor declares that he has taken safeguard measures required under Article 32 of the GDPR, in accordance with Article 28(3) point c of the GDPR. Ensuring data security includes data protection against security breaches leading to breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (personal data breach). When assessing the appropriate level of security, the Parties shall take 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.
7. The Processor declares that he respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor, in accordance with Article 28(3) point d of the GDPR. The Processor shall give 14 days notice of its intention to add or change sub-processors in the form of an announcement on its website, under the "About Us" tab, allowing the Entruster to object to such changes. Adding or changing further processors does not require an amendment to this Agreement.
8. As of the date of the Agreement, the Entruster agrees that the Processor may entrust the processing of personal data to the processors indicated in Annex 1 to the Agreement. Access to certain functionalities of the System may require the consent of the Entruster for further entrustment of personal data.
9. The Processor shall be fully responsible to the Entruster for fulfilling the obligations under the personal data processing agreement entered into between the Processor and the sub-processor. If the sub-processor fails to comply with its data protection obligations, the full responsibility to the Entruster for the fulfilment of the obligations of such sub-processor shall rest with the Processor.
10. The Processor takes into account the nature of the processing, assists the Entruster by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Entruster's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, in accordance with Article 28(3) point e of the GDPR. The Processor is neither entitled nor obliged to respond directly to the requests of the data subjects. If the data subject objects to the processing of personal data for direct marketing purposes, the Processor may stop such processing, which is the implementation of the Entruster's instructions.
11. The Processor assists the Entruster in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Processor, in accordance with Article 28(3) point f of the GDPR. In particular:

11.1. **[Data breach concerning data processed by the Entruster]** In the event of a personal data breach concerning data processed by the Entruster, the Processor shall assist the Entruster:

11.1.1. in notifying the personal data breach to the competent supervisory authority, without undue delay after the Entruster has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

11.1.2. in obtaining the following information which, pursuant to Article 33(3) of the GDPR, shall be stated in the Entruster's notification, and should include:

11.1.2.1. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

11.1.2.2. the likely consequences of the personal data breach;

11.1.2.3. the measures taken or proposed to be taken by the Entruster to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

11.1.3. in complying, pursuant to Article 34 of the GDPR, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

11.2. **[Data breach concerning data processed by the Processor]** In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Entruster without undue delay but no later than 24 hours after the Processor having become aware of the breach. Such notification shall contain:

11.2.1. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

11.2.2. the details of a contact point where more information concerning the personal data breach can be obtained;

11.2.3. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

12. The Processor makes available to the Entruster all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Entrusteror another auditor mandated by the Entruster, in accordance with Article 28(3) point h of the GDPR and under the conditions set out in §5 below.

13. The Processor shall immediately inform the Entruster if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

§5 Audits

1. The Entruster is entitled to carry out, not more than once during each subsequent calendar year, an audit of the security of personal data processing, in terms of compliance of their processing with the PDPA and applicable law, in particular the GDPR.
2. The basic form of auditing is an audit carried out by electronic means. It consists in sending by the Entruster to the Processor questions regarding the compliance of the processing by the Processor of the entrusted personal data with the PDPA, the GDPR or the provisions of generally applicable law on the protection of personal data, including the security measures applied. The Processor is obliged to answer the Entruster's questions, insofar as this is possible, within 30 days of receiving them.
3. After the audit referred to in point 2 above, the Entruster, if necessary, is entitled to conduct an audit in a different form. After receiving a request to conduct such an audit, the Parties will determine the date of its commencement (which may not take place earlier than 30 business days from receipt of the Entruster's request), its exact scope, and persons authorised to conduct it.
4. Audits will be carried out during the working hours of the Processor's business, to the extent and in the area necessary for the processing of personal data, without prejudice to the normal conduct of business by the Processor, the business secrets of the Processor and confidential information belonging to third parties. The Entruster undertakes to keep the above-mentioned information confidential. Before starting the audit activities, the Parties (and an external auditor appointed by the Entruster, if applicable) will sign an appropriate confidentiality agreement.
5. The costs of the audit are borne by the Entruster.

§6 Data transfer outside the European Economic Area

1. **The Processor shall not transfer personal data entrusted by the Entruster outside the European Economic Area.**
2. In situations where the Entruster processes personal data or has an establishment outside the European Economic Area (hereinafter: EEA) and therefore a transfer of personal data is necessary as referred to in §6(1) of the PDPA, the standard contractual clauses referred to in Commission Implementing Decision (EU) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council, with the following content, shall apply:
   a. when personal data is transferred outside the EEA to the Entruster, which is the processor in relation to such data - link,
   b. when personal data is transferred outside the EEA to the Entruster, who is the Controller of such data - link.
3. An amendment to the "List of sub-processors" appendix does not constitute an amendment to the PDPA.
4. If it is necessary to conclude the standard contractual clauses referred to in § 6(2) of the PDPA in written form, the Processor shall forward the request to conclude them in this form to the Processor at dpo@salesmanago.com.
5. In case it is necessary to transfer data to a sub-processor located outside or processing personal data outside the EEA for proper performance of the Agreement, the Processor must ensure that the standard contractual clauses are signed with the sub-processor. Additionally, if any of the Processor's suppliers process data entrusted by the Entruster outside the EEA, they are also obligated to sign the standard contractual clauses for data protection.
6. Standard contractual clauses referred to in §6(2) and §6(5) of the PDPA apply only in the absence of a decision pursuant to Article 45(3) GDPR.

§ 7 Liability

1. Each Party shall be liable for any damage caused to the other Party or to any third parties in connection with the performance of this PDPA, pursuant to provisions of the GDPR or this PDPA.
2. The Processor shall not be responsible for the personal data provided by the Entruster beyond the scope specified in §3(1) of the PDPA unless the Entruster indicates the new scope of data in the Order Form. To avoid any doubts, the Processor shall be responsible for the personal data specified in the Order Form to the same extent as the data specified in §3(1) of the PDPA.
3. In the event of damage caused by actions undertaken by the Processor, the Processor shall be liable as guilty of the actual damage incurred by the Entruster. In no event shall the aggregate liability of the Processor arising out of or related to the PDPA exceed the total amount paid by the Entruster for the services giving rise to the liability in the twelve months preceding the first incident out of which the liability arose. In no event will Processor have any liability arising out of or related to the PDPA for any lost profits, revenues, goodwill, or indirect, special, incidental, consequential, cover, business interruption or punitive damages. The foregoing disclaimer will not apply to the extent prohibited by law.
4. The Processor shall be excluded from liability for adequately securing personal data in accordance with this PDPA in the part of the information system administered by the Entruster.
5. To avoid doubts, if the Processor is responsible for an event due to the Entroster's violation of the law, including failure to obtain or improperly obtain consent for processing personal data, the Processor will not be held liable.

§8 Representatives of the Parties

For the purposes of implementing this PDPA, the Entrusterand the Processor appoint a contact person:

a. The Entruster: contact person indicated in the Order Form
b. The Processor: email: dpo@salesmanago.com
   - the indicated person may be changed at any time via email. Such change does not constitute an amendment to the PDPA.

§9 Final provisions

1. The Processor shall not charge any additional fees for the performance of any of the provisions of this PDPA.
2. This PDPA is concluded for the duration of the Agreement and for the performance of all obligations under this PDPA.

3. In the event of terminating the Agreement, the Entruster shall, within 7 days of the date of expiry hereof, individually secure any personal data entrusted to Processor for processing. 14 days following the date of expiry of the PDPA, the Processor shall permanently delete any and all records containing personal data entrusted for processing, made in connection with or while performing the Agreement. The provisions of Paragraph 9(3) do not apply to data processed by the Processor as part of data backup. Backups are created, in particular, to secure the data and ensure the availability of the data in the course of providing the Service. Backups are kept for a period of 2 years from the date of their creation and are automatically deleted after this period. Personal data shall be processed within the backups in encrypted form, and only authorised persons acting on behalf of the Processor shall have access to such data. This Agreement shall be terminated upon the expiration of the period of data processing as part of data backup.
4. Any issues falling outside the scope of this PDPA shall be governed by the provisions of the GDPR.

List of sub-processors

1. The processor entrusts personal data to the following entities:

No.	Sub-processor	Address	Contact information	Scope of entrusted personal data	Entrusting purpose
1.	Vercom S.A.	ul. Franklina Roosevelta 22 60-829 Poznań	iod@vercom.pl	the phone number, first name, last name, and any other relevant information that is required to fulfil the agreement	Providing SMS messaging services
2.	LINK Mobility Poland sp. z o.o.	ul. Toszecka 101 44-100 Gliwice	dpo@linkmobility.com	the phone number, first name, last name, and any other relevant information that is required to fulfil the agreement	Providing SMS messaging services (entrustment occurs only in the situation specified in §2(1) of the Terms and conditions)

Appendix no. 3 to the Order Form - Information on the processing of personal data for the Customer, persons representing the Customer, Users and contact persons

The data controller: The data controller of your personal data is Benhauer sp. z o.o. based in Cracow entered in the Register of Businesses maintained by Division XI of the National Court Register of the District Court for Kraków-Center in Kraków under KRS number 0000523346, REGON number 122334666 and NIP number 6762447754 (hereinafter referred to as “Benhauer” or “the controller”).

Purposes and legal basis of personal data processing: The controller will process personal data of the contractors who are natural persons:

- to perform an agreement between the contractors and the controller or take action at the request of the contractors before the conclusion of the contract (Article 6(1)(b) of the GDPR);
- fulfilling the legal obligations incumbent on the controller, arising in particular from tax and accounting legislation (Article 6(1)(c) of the GDPR);
- pursuing or defending against claims, which is the legitimate interest of the controller (article 6(1)(f) of the GDPR).

Purposes and legal basis of personal data processing: The controller will process personal data of the contractor’s representatives persons conducting agreements, users and contact person:

- to maintain business contacts, which is the legitimate interest of the controller (Article 6(1)(f) of the GDPR);
- fulfilling the legal obligations incumbent on the controller, arising in particular from tax and accounting legislation (Article 6(1)(c) of the GDPR);
- for the purpose of creating a user account to perform the contract concluded with the customer, which is a legitimate interest of the controller (Article 6(1)(f) of the GDPR);
- pursuing or defending against claims, which is the legitimate interest of the controller (Article 6(1)(f) of the GDPR).

The recipients of the personal data: The controller may disclose the personal data of the contractors to entities authorised by the law. Entities supporting the controller, including IT services providers, may also have access to the personal data of the contractors on the basis of agreements conducted with the controller.

Processing period: The personal data of the contractors shall be processed for the period required by the law or by the limitation period for any claims, depending on which of these events occurs later. The personal data processed for contact purposes will be processed for the time for the duration of the business relationship.

Voluntary/obligation to provide personal data: Providing personal data is voluntary however necessary to conclude an agreement with the controller.

Transfers of personal data to third countries or international organisations: Your personal data will also be processed in tools/systems provided by the entities supporting the data controller that are based or process data outside the European Economic Area. In this case, personal data is transferred on the basis of standard contractual clauses approved by the European Commission or a decision of the European Commission stating an adequate level of protection in a given country, e.g. on the basis of the EU-US Data Protection Framework.

Decision-based solely on automated processing/profiling: The controller is not making decisions based solely on automated processing, including profiling (concerning the purposes of data processing described above).

Data subjects rights: You have the right, as applicable, to:

- request access to your personal data, rectification, deletion and limitation of processing, and if your personal data is processed by automated means on the basis of a contract, you also have the right to transfer your personal data;
- withdraw your consent at any time, if that data was processed on the basis of this consent. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.
- object to the processing of your personal data - when the data is processed on the basis of the controller's legitimate interest.
- You also have the right to lodge a complaint with the supervisory authority (PUODO - President of the Office for Personal Data Protection) Stawki 2 st., 00-193 Warszawa, email: kancelaria@uodo.gov.pl

The data controller:
Benhauer sp. z o.o. based in Cracow
Stanisław Klimecki 4 st.
30-705 Kraków
e-mail: rodo@salesmanago.com

Data Protection Officer:
e-mail: dpo@salesmanago.com

Appendix no. 4 to the Order Form - Anti-spam Policy

Valid from 1 March 2024

ANTI-SPAM POLICY OF VERCOM S.A.

§ 1. GENERAL PROVISIONS

1. This Anti-Spam Policy sets forth the minimum standards for using the Services rendered by Vercom via electronic means put in place in order to protect the Message recipients from unwanted or unlawful SPAM or Smishing communication.
2. This Anti-Spam Policy constitutes an integral part of the Framework Agreement on the Provision of Services by Electronic Means („Agreement”). In matters not covered by the Anti-Spam Policy, the remaining contractual documents, particularly the provisions of the Agreement, shall apply to it.
3. Vercom is a telecommunications enterprise listed in the register of SMS service integrators maintained by the President of the Office of Electronic Communications (President of the OEC) in accordance with the Act of July 28, 2023, on combating abuse in electronic communication.
4. Message recipients who have received SPAM or Smishing communication may seek support by reaching Vercom at: abuse@redlink.pl.

§ 2. DEFINITIONS.

For the purposes of this Anti-Spam Policy, the following definitions shall apply:

1. SPAM – any communication of a commercial character, sent to the end-user without their prior, verifiable consent;
2. Smishing – sending a Message, including a short text message (SMS), in which the sender impersonates another entity to prompt the recipient of the Message to engage in specific actions, particularly disclosing personal data, unfavourable disposition of property, opening a website, initiating a voice call, or installing software;
3. Sending of Messages (including the lower case spelling) – sending Messages utilising the Services rendered by Vercom.
4. Client - a natural person, a legal person or an organisational unit that is not a legal person to which a separate act grants legal capacity, not being a consumer, who has concluded the Agreement with Vercom.
5. NASK - Computer Security Incident Response Team of the Research and Academic Computer Network - National Research Institute.
6. Services - the services provided by Vercom to the Client under the Agreement.
7. Override - Sender ID replacing the MSISDN number in the SMS/MMS sender field.
8. NASK List - a list containing the contents of Smishing message templates developed by NASK,
9. Public Entity - the public entities identified in the Act of July 28, 2023, on combating abuse in electronic communication.

§ 3. SERVICES DEDICATED TO PROFESSIONALS.

In order to minimise the risk of exposure of clients to SPAM or Smishing:

1. The Agreement may only be concluded with professional entities - entrepreneurs and public entities. Additionally, an entrepreneur who is a natural person may conclude such an Agreement only if it is directly related to his or her business activity and has a professional character for him or her, resulting in particular from his or her business activity, made available on the basis of the provisions on the Central Registration and Information on Business;
2. Sending Messages to actual recipients (outside the Client’s own personal data) may take place only after a positive verification of the Client performed by Vercom.
3. The sending of a Message of a Public Entity may be commissioned to Vercom directly by that Public Entity or by a third party commissioning the sending on behalf of and for the Public Entity.
4. A Client ordering the dispatch of a Message on behalf of and for a Public Entity shall, prior to the commencement of that order, provide Vercom with a statement from the Client and the Public Entity as to the right to dispatch Messages on behalf of that Public Entity.
5. In the event that the Client's right to order the sending of Messages on behalf of and for a Public Entity expires, the Client shall, within 1 business day, notify Vercom of this.

A Client commissioning a Message on behalf of a public entity shall in each case send Vercom the name and REGON of the public entity for which the client is commissioning the Message.

§ 4. END-USERS.

1. The Client shall be fully liable for the lawfulness of sending Messages to a specific recipient. In particular, the Client is obliged to obtain all necessary, prior and verifiable consents in this respect, as well as to register them appropriately. The consent of the recipient must be clear and unambiguous, and may not be implied or derived out of any other content or declaration, in any way. In addition, the recipient must be entitled to a simple, unhindered withdrawal of consent at any time, in a way at least as easy as the way the consent has been granted. Sending Messages to recipients who have withdrawn their consent to receive them is prohibited. Vercom shall not be liable for the correctness, lawfulness and the way of collecting consents from the users.
2. Vercom has the right to introduce a non-removable registration link in each Message, enabling the recipient to withdraw the consent to receive Messages.
3. Using publicly available contact data of the recipients, in particular collected from: websites acquired under any title of databases or collected using hidden methods is prohibited. The first sentence shall also apply to contact details of addressees who are legal persons and organisational entities without legal personality and Public Entities
4. All kinds of automated solutions, software or scripts for the collection of contact data are prohibited.

5. Vercom has the right to verify the sendings carried out by the Client in terms of meeting the characteristics of SPAM or Smishing, as well as in terms of the existence of spam traps and the number of bounces, after the Client's sending. A negative result of such verification, including obtaining information about violations of legal requirements regarding required consents and permissions, entitles Vercom to terminate the Agreement with immediate effect.

§ 5. CONTENT OF MESSAGES.

1. It is forbidden to send Messages with any content that is unlawful, inciting to commit unlawful acts, discriminatory, insulting or offensive to third parties, inciting to hatred, vulgar and pornographic.
2. Sending SPAM or Smishing messages is prohibited.
3. The Client is obliged to include in the Messages true and accurate information regarding the sender and the subject. It is forbidden to indicate the sender or the subject or the content of the Message in a misleading way or even suggesting the facts other than true.
4. It is forbidden to use in Override of SMS / MMS messages, content that may mislead the addressee about the identity of the sender, in particular unauthorised use of names, names of institutions, companies and trademarks.
5. It is forbidden to use in Override of SMS / MMS messages commissioned by entities that are not Public Entities, content included in the NASK List of Associations of Public Entities, as well as content compliant with with variants of the name or abbreviation included in the NASK List of Overrides of Public Entities.
6. The Message of a Public Entity must contain an Override in the form of a name or its abbreviation reserved for that Public Entity in the NASK List. In the event that the Public Entity commissioning Vercom directly or indirectly to send the Message does not have an Override reserved in the NASK List, the Message of this Public Entity may not contain Overrides reserved for other Public Entities and Override in the form of name variants or abbreviations that may mislead the recipient as to the origin of the Message from the Public Entity in the NASK List.
7. It is forbidden for non-Public Entities to send Messages with an Override containing the phrase #RP.
8. The Client is solely responsible for the content of the Messages sent. Vercom shall not be liable for the content sent by the Client within the use of the Service.

§ 6. MAILING POLICY

1. The Client is obliged to take care of the database intended for sending of Client's Messages (i.e., in particular for verifying data validity, removing data that are duplicated, obsolete, incorrect or inactive, appropriate data segmentation, etc.) and maintaining statistics of sending EMAIL Messages below the permissible below the permissible thresholds for the status of EMAIL messages (hereinafter: Thresholds) mentioned in section 2. In the event of exceeding the Thresholds specified in section 2 above, Vercom is authorised to suspend or close the Account. Vercom will contact the Client prior to suspension or closure of the Account in order to explain the reasons of its decision, unless the risk associated with further handling of sending is considered critical to the security of the Vercom services. Suspension or termination of the Account is the ground for termination of the Agreement by each of the Parties for reasons attributable to the Client.
2. Vercom applies acceptable Thresholds in accordance with the table below. Thresholds are calculated as the percentage share of EMAIL Messages with a specified status in comparison with all EMAIL Messages sent from a given Account within 24 hours. The Thresholds below do not pertain to SPAM or Smishing Messages, which are not allowed.

Sent EMAIL Message Status	Permitted Vercom anti-spam thresholds
Hardbounces	≤ 10%
Spambounces	≤ 2%
Spam Complaints	≤ 0.1%
Unjustified abuse complaints	< 1

Definitions of terms used in the table above:

a) Hardbounces - when EMAIL Message has not been delivered as the address or domain does not exist or the recipient blocks the delivery of EMAIL Messages;

b) Spambounces - when EMAIL Message has been classified as spam in the recipient's mailbox;

c) Spam Complaints – when the recipient of the EMAIL Message has marked it as spam;

d) Unjustified Abuse Complaints – when the recipient of EMAIL reports that the sender contacts it without the required consent.

3. Vercom and its cooperating telecommunications companies block the sending of a Message whose content matches with the content of the Message template contained in the NASK Listor which contains Overrides referred to in the prohibition from § 5.
4. Vercom and its cooperating telecommunications entrepreneurs may block a Message whose content includes Smishing, other than match with the content of the Message template in the NASK List, including MMS.
5. Vercom blocks the provision of Services to the Client in whole or in part if the President of UKE issues an administrative decision under Article 23 of the Act on Combating Abuses in Electronic Communication instructing the introduction of such a block, and will promptly inform the Client thereof. Such blocking shall not constitute a breach of the Agreement or grounds for the Customer to terminate the Agreement.
6. Vercom may charge for sending a Message that has been blocked in accordance with clauses (3) and (4), in particular where the Message has been blocked by a cooperating trader.
7. Vercom shall not be liable for the blocking of a Message pursuant to clauses 3 and 4, in particular such blocking shall not constitute a breach of the Agreement or grounds for the Customer to terminate the Agreement.

§ 7. FINAL PROVISIONS.

1. The Client shall be fully and solely responsible for the compliance of the sending of the Message with the applicable law, the Agreement and the rules specified in the Anti-Spam Policy. If the Vercom is to bear any liability (civil, administrative, criminal or other) resulting from the Client’s breach of the obligations specified in the first sentence, the Client shall be liable to Vercom on the basis of recourse for any damage, including lost profits resulting therefrom, as well as any potential financial sanctions applied to Vercom by the President of the Office of Electronic Communications.
2. In the event of a breach by the Client of any of the obligations specified in the Anti-Spam Policy, Vercom is entitled to terminate the Agreement with immediate effect.
3. Vercom will collect and process information related to the Service, including the content of the Message that has been blocked as Smishing or because of the use of Overrides which do not comply with § 5, for a period of 12 months from the date on which the Service was to be provided or for the period necessary to resolve a dispute arising from the blocking of the Service.
4. For the purpose of identifying, preventing, and combating abuses in electronic communication, Vercom will provide NASK and other telecommunications entrepreneurs with information related to the Service, excluding the content of a message that has been identified by Vercom as other than Smishing as a form of abusive electronic communication.
5. The provisions of clauses 3, 4 and 5 shall exclude the application of the confidentiality principle from the Agreement.