SALESıɪlmanago

MAIN SERVICES AGREEMENT

Effective date: 12.09.2025

This Main Services Agreement (MSA) governs Customer's acquisition and use of SALESmanago services. Capitalised terms have the meaning as set forth in the definitions herein.

By accepting this Main Services Agreement or by executing an Order Form that references this MSA, Customer agrees to the terms of this MSA. If the individual accepting this MSA is accepting on behalf of a company or other legal entity, such individual represents that they have the authority to bind such entity to these terms and conditions, in which case the term "Customer" shall refer to such entity. If the individual accepting this MSA does not have such authority or does not agree with these terms and conditions, such individual must not accept this MSA and may not use the services.

I. DEFINITIONS

1. "**Account**" means an account enabling the use of the Services, understood as the use of a selected package.
2. "**Active Contact**" means a contact within the Customer's or the end-customer's website database who meets at least one of the following criteria within 180 days:
   a. E-mail Communication Permission: The contact has explicitly granted permission to receive email communications from the Customer or the end-customer;
   b. SMS Communication Permission: The contact has explicitly granted permission to receive SMS (text message) communications from the Customer or the end-customer;
   c. Web Push Permission and Profile Creation: The contact has:
      i. Granted permission to the Customer or the end-customer to receive web push notifications from the Customer or the end-customer;
      ii. A profile that has been successfully created within the SALESmanago platform;
   d. Recent Purchase Activity: The contact has registered an external event of type "Purchase" within the past 180 days;
   e. Recent Cart Activity: The contact has registered an external event of type "Cart" within the past 180 days.
3. "**Additional Fee**" means the sum of money that SALESmanago may charge the Customer in the event the Customer terminates the Agreement using the Maximum Notice Period, corresponding to the sum of the Customer's fees for the use of the System for the remaining term of the Agreement had it not been terminated. The Additional Fee does not apply if the Customer terminates the Agreement due to circumstances for which SALESmanago is liable.
4. "**Agreement**" means the agreement concluded between the Customer and SALESmanago on the basis of the Order Form and the MSA.
5. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Party. The definition also includes "related parties" within the meaning of the Polish Act of 29 September 1994 on accounting.
6. **"Confidential Information"** means all confidential information disclosed by either Party ("Disclosing Party") to the other Party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood as confidential given the nature of the information and the circumstances of disclosure. However, Confidential Information will not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party (including its directors, officers, employees, contractors or agents) prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.
7. "**Customer**" means the individual, a company or other legal entity which has entered into Order Forms.
8. **"Data Act"** means Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

9. **"GDPR"** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

10. "**ICT**" means information and communication technologies referred to in the Data Act.

11. "**Information on jurisdiction**" means the information on the jurisdiction to which the ICT infrastructure deployed for data processing within SALESmanago's individual services is subject, as referred to in Article 28 (1) (a) of the Data Act - contained in Appendix 4 to the MSA.

12. "**Maximum Notice Period**" means a period of two calendar months.

13. "**Maximum Transitional Period**" means the period of 30 calendar days initiated after the Maximum Notice Period.

14. "**MSA**" means this Main Services Agreement.

15. "**Onboarding Services**" means the Services, including implementation Services, provided to the Customer in accordance with the Terms of Onboarding Services, attached as Appendix no. 3 to the MSA.

16. "**Order Form(s)**" means an ordering document specifying the Services to be provided under said document that is entered into between Customer and SALESmanago, including any annexes and supplements to it.

17. "**Parties**" means the Customer and SALESmanago.

18. "**Password**" means a sequence of signs, including alphanumeric, necessary to perform an authentication process while accessing the Account, determined by the User during the registration process.

19. "**Personal Data Protection Regulations**" means the regulations regarding processing of Personal Data including GDPR and The Personal Data Protection Act.

20. "**Personal Data**" means any information relating to an identified or identifiable natural person according to the Personal Data Protection Regulations.

21. "**Retrieval Period**" - the period of data retention by SALESmanago of at least 30 calendar days, beginning after the end of the transitional period agreed between the Customer and SALESmanago in accordance with the Data Act.

22. "**SALESmanago**" means Benhauer sp. z o. o. based in Cracow, address: ul. Stanisława Klimeckiego 4, 30-705 Kraków, NIP: 676 244 77 54, entered into the Register of Entrepreneurs of the National Court Register kept by the District Court for Kraków Śródmieście in Kraków, XI Commercial Division of the National Court Register under KRS entry: 0000523346, with a share capital in the amount of PLN 1 407 450.00.

23. "**Services**" means the services that are ordered by Customer under an Order Form and made available online by SALESmanago including electronic services within the meaning of the Electronic Provision of Services Act of 18 July 2002 (Dz.U.2020.344 t.j., with subsequent amendments) which consist in: (i) providing the User an Account and (ii) enabling to use the System through the Account, including providing the User profile.

24. "**System**" means the online Customer Engagement Platform.

25. "**The Personal Data Protection Act**" means the Act of 10 May 2018 on the Protection of Personal Data (Dz.U. 2019.1781 t.j. with subsequent amendments).

26. **"Third Party Provider"** means a provider of Third Party Services approved by SALESmanago.

27. **"Third Party Services"** means the services provided by a Third Party Provider to Customer in connection with the use of the System.

28. "**User profile**" means an arrangement that can store information, made available by SALESmanago within the ICT system, that enables the User to enter, store and modify data necessary for proper usage of the features of the System. This information is provided to the System voluntarily and solely by the User.

29. "**User**" means a natural person above 18 years of age with legal capacity who uses Services on behalf of the Customer.

II. SUBJECT MATTER OF THE MSA

1. SALESmanago grants the Customer a non-exclusive, non-transferable right and licence to use the System available at www.salesmanago.com, which collects behavioural and transactional data about the Customer's clients and delivers personalised communications across all marketing channels.

2. SALESmanago will provide Services described in the Order Form, including Onboarding Services (if applicable).

3. SALESmanago may, at its own discretion, temporarily provide the Customer with additional functionalities of the System free-of-charge (hereinafter referred to as "Additional Functionalities"). Customer agrees that SALESmanago, in its sole discretion and for any or no reason, may terminate Customer's access to the Additional Functionalities or any part thereof. Customer agrees that any termination of Customer's access to the Additional Functionalities may be without prior notice, and Customer agrees that SALESmanago will not be liable to Customer or any third party for such termination. Notwithstanding the "Liability" section below, the Additional Functionalities are provided "as-is" without any warranty and SALESmanago shall have no

indemnification obligations nor liability of any type with respect to the Additional Functionalities unless such exclusion of liability is not enforceable under applicable law in which case SALESmanago's liability with respect to the Additional Functionalities shall not exceed EUR 100.

4. In the event that the Customer decides to enter into an agreement regarding the sending of SMS messages, the terms and conditions available [here](#)[1] will apply.

III. CUSTOMER SERVICE AND TRAINING

1. The Customer can use the support Service available at support@salesmanago.com with a maximum response time of 24 hours free-of-charge.
2. SALESmanago enables the Customer to participate in free weekly online training on the use of the System carried out by SALESmanago Specialists.

IV. RESPONSIBILITIES OF THE PARTIES

1. SALESmanago will provide Services with the due diligence required.
2. Each Party agrees to keep in confidence any Confidential Information disclosed by the other Party, not to use any Confidential Information belonging to the other Party for any purpose outside the scope of the Agreement and to limit access to Confidential Information to those of its directors, officers, employees, contractors, subcontractors and agents who need such access for the purpose of the Agreement. The confidentiality obligations shall remain in effect for the term of the Agreement and 5 years after its termination. Either Party may disclose Confidential Information if it is compelled by the applicable law to do so, provided it gives the other Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance to contest the disclosure. SALESmanago reserves the right to share data, including Confidential Information, with its Affiliates for commercial purposes including analysis, compilation of summaries or marketing or sales activities (including offering) subject to an obligation of confidentiality under similar conditions.
3. The Customer is obliged to use the System in compliance with the rules of law and in good faith, including compliance with SALESmanago Marketing Automation Anti-Spam Policy as described below.
4. While using the Services, the Customer is obliged, in particular to:
   a. use the System in a way that does not violate the SALESmanago's intellectual property rights, especially in a way that does not distort its functioning, in particular through the use of certain software or devices;
   b. keep the Password secret and make every effort to prevent third parties from gaining possession of the Password; and
   c. not using the System for the purpose of any illegal activity.
5. The Customer is responsible for:
   a. any User's use and/or misuse of the Service;
   b. the legality, reliability, integrity, accuracy and quality of its data; and
   c. the integration between its resources and the System.
6. The minimum technical requirements which enable using the Services and/or the System are as follows:
   a. Services available through the Customer's website (widgets): any modern browser which supports HTML5, CSS3, JavaScript, cookie files, LocalStorage, Web Push notifications, and is not restricted from accessing the resources located on SALESmanago infrastructure.
   b. Services available through salesmanago website (admin panel): access to the internet, the latest version of one of the following web browsers: Google Chrome, Mozilla Firefox with a default configuration.
7. At the time of signing the Agreement, the System is compatible with the above requirements. Temporary incompatibility may result from changes made by third-party vendors. SALESmanago will exercise due professional care in ensuring the continued compatibility of the System.
8. The Customer may choose to obtain Third Party Services to use with features within the System (e.g. applications) and/or for implementation or onboarding service. In this regard, the Customer will be required to obtain access to Third Party Services from Third Party Providers. The Customer agrees to comply with the terms and conditions of the Third Party Services and the policies and guidelines pertaining thereto. Notwithstanding the foregoing, SALESmanago does not assume any responsibility for the Third Party Services, the terms of which have been regulated directly between the Customer and the Third Party Provider and specifically disclaims any liability, warranty, and obligation with respect to such Third Party Services, whether or not it is recommended or approved by SALESmanago, or otherwise noted.

---

[1] https://www.salesmanago.com/marketing-automation/salesmanago-order-form-sms.htm

SALESmanago may terminate the cooperation with any Third Party Provider at any time without reason or change the Third Party Provider and such change shall not constitute a breach of the Agreement. SALESmanago assumes no responsibility for: (i) claims arising from the combination of any Services with any other products, services, hardware, data or business processes or use of Services by Customer other than in accordance with the Agreement; and (ii) for any amendment or modification to the Services not carried out by SALESmanago or one of its approved partners.

9. The Customer shall only use the Services for its own internal business operations. The Customer acknowledges and agrees that it will not allow any third party, including Customer's vendors and service providers, to access or use the Services unless such third party is allowed access for the purpose of providing authorised customer support services or in connection with Customer's appropriate use of the Services for its business purposes.

10. SALESmanago reserves the right to temporarily or permanently restrict the functionality of the System in the event that the Customer violates generally applicable laws or the Agreement (and this restriction does not affect the remuneration payable to SALESmanago).

11. SALESmanago reserves the right to suspend the dispatch of messages planned by the Customer via the System when:
    a. there is a risk that a significant decrease in the deliverability of messages sent via the SALESmanago will occur in connection with that dispatch, or
    b. the dispatch will or may adversely affect the reputation of SALESmanago's dispatch servers, or
    c. the dispatch will or may negatively affect the reputation of the SALESmanago brand, or
    d. the dispatch does not comply with generally accepted good email marketing practices including SALESmanago Marketing Automation Anti-Spam Policy as described below.

12. SALESmanago for security reasons, reserves the right to block any Account in the System that has not been logged in correctly for a period of 2 years (and this restriction does not affect the remuneration payable to SALESmanago). The Customer will be informed well in advance if the account is to be blocked for this reason.

13. For some of the System's functionalities, there may be quantitative and qualitative limits specified in the System (e.g. a certain number of uses per month). If the specified limit is reached, the respective functionality may not be available until the conditions for the provision of a new limit are met. Concurrently, the Customer agrees that, where applicable, an additional paid limit shall be automatically triggered upon reaching the assumed limit, without requiring further confirmation from the Customer.

V.   FEE AND PAYMENTS

1. The Customer will be charged a fee for the Services under the detailed price list described in the Order Form. Some fees may be calculated on the basis of the number of contacts or Active Contacts, which shall be determined in the Order Form.

2. The terms of payment for Services are described in the Order Form. Invoices will be issued at the end of each first month of the settlement period. Unless the Order Form states otherwise, the settlement month corresponds to the calendar month, and for an incomplete month of using the System, the remuneration is determined proportionally.

3. Fees indicated in the Order Form will be increased by the indicated value on each anniversary of the entry into force of the Agreement in the form of an Annual Innovation Premium. The beforementioned fee increase does not require an amendment to the Agreement. The indexation rate is:
    a. for fees in euro - increase in the annual Harmonised Index of Consumer Prices (HICP) of the euro area (inflation in the euro area) announced by Eurostat +3% with a minimum of 5%;
    b. for fees in US dollars - increase in the annual Consumer Price Index (CPI) announced by the Bureau of Labor Statistics +3% with a minimum of 5%.

4. If during the term of the Agreement the Customer reaches a given threshold of the number of contacts or Active Contacts in the System database, indicated in the Order Form, the charge for this threshold becomes the minimum commitment monthly amount for the Customer under the Agreement in terms of the fee depending on the number of e-mail contacts / Active Contacts stored in the System database.

5. Except as otherwise specified herein or in an Order Form, (i) fees are based on the number of contacts / Active Contacts stored in the System database and not actual usage of the System, (ii) payment obligations are non-cancelable and fees paid are non-refundable.

6. 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).

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.

VI. COMPLIANCE

1. The Customer shall comply with all applicable export controls, economic sanctions, and import laws and regulations, including without limitation the regulations of the European Union, United Kingdom, and the United States, as in force and amended from time to time. This means that Customer will not, directly or indirectly enter into a business relation with any person or entity resident in, located in, or organised under the laws of any country or territory subject to comprehensive economic sanctions (including, currently, Crimea, Cuba, Iran, North Korea, and Syria) (hereafter "Sanctioned Countries"), or (ii) identified on any applicable restricted party lists (including without limitation the U.S. Treasury, Office of Foreign Assets Control's Specially Designated Nationals List; the HM Treasury Consolidated List of Financial Targets in the UK; and the European Union's Consolidated List of Sanctioned Individuals and Entities) (hereafter "Restricted Party Lists").
2. The Customer warrants that it is, and will remain during the term of this Agreement, not (i) resident in, located in, or organised under the laws of a Sanctioned Country, or (ii) identified on, or majority-owned or controlled by one or more parties identified on, a Restricted Party List. SALESmanago reserves the right to request the Customer to periodically confirm in writing that it complies with the obligation under the Agreement and specifically with those in this section VI, Compliance.

VII. 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. 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.
2. SALESmanago will not be responsible for delays, delivery failures or other loss resulting from the transfer of Customer's data over communications network or facilities, including the internet.
3. If the Service are held or are likely to be held infringing intellectual property rights of a third party, SALESmanago will have the option, at its expense to (i) replace or modify the Services as appropriate, (ii) obtain a licence for Customer to continue using the Services, (iii) replace the Services with a functionality equivalent service or (iv) terminate the applicable Services and refund any prepaid charges applicable Services following the effective date of termination. To the fullest extent permitted by law, remedies described in the preceding sentence will constitute the sole and exclusive remedy available to Customer in relation to third party claims.
4. Without prejudice to the foregoing, SALESmanago's liability arising out of or in connection with the Agreement shall be excluded to the extent that the Customer has suffered damage due to a failure to comply with certain industry requirements applicable to the Customer's business (e.g. arising from the provisions of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011); hereinafter "DORA") of which SALESmanago has not been informed in advance and SALESmanago declared that it will meet these requirements to the extent they apply to SALESmanago.
5. To the maximum extent permitted by applicable law, the Services including all functions thereof, are provided on an 'as is' basis, without representations or warranties whether express, implied or otherwise, including any implied warranty of merchantability or fitness for a particular purpose.

VIII. TERM AND TERMINATION

1. The Agreement enters into force on the date and for a fixed period indicated in the Order Form and will automatically renew for successive periods indicated in the Order Form unless terminated by the Customer in writing at least 30 days before the end of the Agreement.
2. The Customer has the right to terminate the Agreement if the main System's features remain unavailable for consecutive 7 days from receiving the notification from the Customer.
3. The Customer has the right to terminate the Agreement with the Maximum Notice Period at any time. In such a case, SALESmanago is entitled to charge an Additional Fee.
4. SALESmanago has the right to terminate the Agreement in the following cases:

    a. the Customer's failure to pay invoices by more than 30 days; or

    b. violation by the Customer of the fundamental rules of social coexistence or business ethics having an impact on SALESmanago's image or SALESmanago brand in particular violation of the SALESmanago Marketing Automation Anti-Spam Policy available **here**[2]; or

    c. breach by the Customer of the rules of law or any material obligation under this Agreement;

    d. violation by the Customer of the business ethics in communication with SALESmanago (in particular abusive behaviour).

5. SALESmanago has the right to terminate the Agreement without reason effective at the end of the current Agreement term, and in the case of Agreement of indefinite duration, with three months' notice.

6. Declaration of termination of the Agreement by the Customer must be, under pain of invalidity, sent: (i) by e-mail to support@salesmanago.com or (ii) by mail to the address of the SALESmanago's registered office. The declaration of termination of the Agreement for its effectiveness must be submitted by a person authorised to represent the Customer.

7. In the event of termination of the Agreement by SALESmanago for reasons attributable to the Customer, SALESmanago shall be entitled to charge a contractual penalty in the amount corresponding to the unpaid portion of SALESmanago's remuneration under the current Agreement term based on the remuneration from the last month before the termination times: (i) the Agreement duration till end of the Agreement or (ii) next renewal date or (iii) three months (for agreements on indefinite duration). The charging of contractual penalty does not exclude SALESmanago to claim the deficiency compensation transferring the amount of withheld contractual penalty. The Customer will be obliged to pay the contractual penalty within 7 days from the date of receipt of the debit note to the bank account indicated in the note.

8. The above breaches, in the event of a written notice to the other Party, result in the immediate termination of the Agreement along with the cessation of the provision of Services to the Customer, and the Customer is obliged to pay remuneration to SALESmanago for each day on which the service was performed.

9. The Order Form prices can contain the Terms Discount.

    In the event of termination of the Agreement by the Customer or by SALESmanago for reasons attributable to the Customer before the expiration of the term for which the Agreement - related to the granting of the discount to the Customer - has been concluded, SALESmanago shall be entitled to claim reimbursement of the discount granted to the Customer less its pro rata value for the period from the date of conclusion of the Agreement until the date of its expiration. The Customer will be obliged to return the relief granted to the Customer in the amount indicated in the preceding sentence within 7 days from the date of receipt of the debit note to the bank account indicated in the note.

IX.   PROCEDURE FOR REPORTING IRREGULARITIES AND COMPLAINT PROCEDURE

1. During the use of the Services, the Customer is obliged to immediately notify SALESmanago of any irregularities, malfunctions, or interruptions in the functioning of the Services or the System, as well as any deficiencies in the quality of the Services, no later than 14 days from the date of becoming aware of such irregularities.

2. Notifications in this respect should be addressed to SALESmanago via email to: support@salesmanago.com.

3. In the case of technical problem reports related to the System, the Customer must obtain confirmation from the SALESmanago Support department that the cause of the reported problem lies with SALESmanago before submitting any complaint as mentioned below. The Customer may file a complaint regarding technical problems related to the System within 14 days from the date of confirmation by the SALESmanago Support department that the cause of the reported problem lies with SALESmanago.

4. Customers' complaints regarding SALESmanago's improper performance of any contractual provisions should include, in particular:

    a. full registration name of the Customer;

    b. address details;

    c. TAX ID number;

    d. login;

    e. the contact details of the User and Customer;

    f. detailed description of the circumstances giving rise to the Customer's complaint;

    g. duration of the irregularities (e.g. error);

    h. description of the complainant's request;

    i. signature and position of the person reporting the incident who is authorised to do so.

5. A response to the complaint will be provided electronically or possibly by telephone.

---

[2] https://www.salesmanago.com/marketing-automation/salesmanago_marketing_automation_anti-spam_policy.htm

6. The complainant will be notified of the outcome of the considered complaint by e-mail to the e-mail address provided in the complaint application within 30 (thirty) days from the date of submission of a complete and correct complaint, with the proviso that the deadline may be extended in particularly complicated cases. Exceeding the deadline for responding to the complaint does not constitute recognition of the complaint.
7. The Customer has the right to appeal the decision on the complaint once within 14 days of receiving the response to the complaint. The above provisions shall apply accordingly.

X. COOPERATION WITH THE AFFILIATES

1. The Customer may enter into agreements regarding the use of products or services of the Affiliates of SALESmanago, in particular Leadoo Marketing Technologies Ltd, 2922046-1, based in Helsinki, Finland.
2. To the extent that there is integration between the System and the products or services of the Affiliates (e.g. in terms of monitoring code, transferring data to and from the System, linking the System's functionalities with products or services of the Affilates), the Parties indicate that this is done at the direction of the Customer.
3. The Customer agrees to comply with the terms and conditions of the Affiliates and the policies and guidelines pertaining thereto. Notwithstanding the foregoing, SALESmanago does not assume any responsibility for the Affiliates, the terms of which have been regulated directly between the Customer and the Affiliates and specifically disclaims any liability, warranty, and obligation with respect to such Affiliates.

XI. PROCEDURE FOR CHANGING SERVICE PROVIDER

1. The Customer, upon its request, is allowed by SALESmanago to switch the provider of services covered by the Agreement to a different provider of data processing service or to port all exportable data and digital assets, referred to in the Data Act, to an on-premises ICT infrastructure, without undue delay and in any event not after the mandatory Maximum Transitional Period, during which the service contract remains applicable. SALESmanago shall in this case:
    a. provide reasonable assistance to the Customer and third parties authorised by the Customer in the switching process;
    b. act with due care to maintain business continuity, and continue the provision of the functions or services under the Agreement;
    c. provide clear information concerning known risks to continuity in the provision of the functions or services on the part of the source provider of data processing services;
    d. ensure that a high level of security is maintained throughout the switching process, in particular the security of the data during their transfer and the continued security of the data during the Retrieval Period, in accordance with applicable Union or national law.
2. SALESmanago supports, to the extent resulting from the Data Act, the Customer's exit strategy relevant to the contracted services, including by providing all relevant information.
3. The Agreement shall be considered to be terminated and the Customer shall be notified of the termination, in one of the following cases:
    a. where applicable, upon the successful completion of the switching process;
    b. at the end of the Maximum Notice Period, where the Customer does not wish to switch but to erase its exportable data and digital assets upon Service termination.
4. SALESmanago shall erase all exportable data and digital assets generated directly by the Customer, or relating to the Customer directly, after the expiry of the Retrieval Period or after the expiry of an alternative agreed period at a date later than the date of expiry of the Retrieval Period, provided that the switching process has been completed successfully.The Parties agree that, due to technical limitations, all exportable data and digital assets generated directly by the Customer or directly relating to the Customer will be erased when they are no longer necessary, not later than after 12 months after the completion of the switching process, unless Parties agree otherwise.
5. The Customer may notify SALESmanago of its decision to perform one or more of the following actions upon termination of the Maximum Notice Period:
    a. switch SALESmanago to a different provider of data processing services, in which case the Customer shall provide the necessary details of that provider;
    b. switch to an on-premises ICT infrastructure;
    c. erase its exportable data and digital assets.

6. Where the mandatory Maximum Transitional Period is technically unfeasible, SALESmanago shall notify the Customer within 14 working days of the making of the switching request, and shall duly justify the technical unfeasibility and indicate an alternative transitional period, which will not exceed seven months. Service continuity shall be ensured throughout the alternative transitional period.
7. The Customer has the right to extend the Maximum Transitional Period once. In this case, the Customer and SALESmanago will enter into negotiations to agree on an appropriate transitional period, taking into account all relevant and reasonable circumstances.

XII.   MISCELLANEOUS

1. The Customer authorises SALESmanago to use the Customer's name and trademark (or logo) to represent the fact that the Customer is a customer of SALESmanago, especially for the purpose of informing about using the System on its website and social media channels.
2. SALESmanago may at any time make any change to any Service that is necessary to comply with applicable law. The names of the System functionalities may change over time and such a change does not constitute an amendment to the Agreement. SALESmanago may make commercially reasonable updates to the Services from time to time to which the Customer agrees on beforehand. SALESmanago will inform Customer via the System if SALESmanago makes a material change to the Services that has a material impact on Customer's use of the Services.
3. SALESmanago may make changes to URLs in the Agreement from time to time. SALESmanago may amend the MSA for important reasons, which are: a) changes in generally applicable laws affecting the provisions of the MSA; b) the issuance of a judgement or decision directly affecting the provisions of the MSA by a court or public administration authority; c) introduction of new functionalities of the System or changes to them; d) removal of ambiguities or doubts of interpretation. In case of the amendment of the MSA, SALESmanago shall notify the Customer of the change by the message that will be communicated to the User via the System.The Parties agree that the User is authorised to accept or reject the new terms and conditions on behalf of the Customer. Failure to respond to information about the change in the MSA within 14 days from the date of notification of the change is considered acceptance of the new terms and conditions. If the Customer objects to the new terms and conditions, the Parties will negotiate the terms and conditions in good faith, but the Customer may not object to changes resulting from the reasons indicated in (a) and (b) above. Customer's objection to the new terms and conditions for reasons other than those indicated in (a) and (b) above means that the existing MSA applies to the performance of the Agreement, whereby, this provision does not affect the Customer's right to terminate the Agreement in accordance with the Data Act, without incurring costs.
4. Any limitation or modification which SALESmanago is entitled to make under the Agreement shall not affect the assessment of the SALESmanago's due performance under the Agreement and does not affect the remuneration payable to SALESmanago under the Agreement.
5. SALESmanago hereby declares that it has a status of a large enterprise within the meaning of Article 4 point 6 of the Polish Act of March 8, 2013 on Counteracting Excessive Delays in Commercial Transactions (Journal of Laws of 2023, item 1790, as amended).
6. According to the Personal Data Protection Regulations, Parties have regulated the principles of entrusting the processing of Personal Data, in the agreement constituting Appendix No. 1 to the MSA. Appendix No. 1 shall apply when the performance of the Agreement involves the processing of personal data to which the provisions of the GDPR apply.
7. 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.
8. SALESmanago implements the information obligation to representatives and employees whose data is listed in the Agreement through the information clause, attached as Appendix 2 to the MSA.
9. Persons representing the Customer acknowledge receipt of information regarding processing their personal data in connection with the Agreement. The Customer agrees to provide this information to employees and associates not mentioned in the content of the MSA, whose data will be transferred between the Parties to perform the Agreement.
10. SALESmanago will be entitled to use data processed as part of the Services to produce: statistical analyses, insights, market data and predictive models to assist development of SALESmanago Services and third

party products or services designed for use with them (hereinafter referred to as the "Analytics"). No Personal Data is used for the purpose of Analytics nor will Analytics identify Customer.

11. 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.

12. Subject to the provisions of the MSA stating that it 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. DocuSign) or in the form of a scanned document. Otherwise null and void. The Parties exclude the application of Art. 66^1 § 1-3 of the Polish Civil Code. A change in the Customer's invoice data, which arises by operation of law, does not require an amendment to the Agreement.

13. If any provision of the MSA is held by a court or other competent authority to be unlawful, void or unenforceable, it shall be deemed to be deleted from the MSA. It shall be of no force and effect, and the MSA shall remain in full force and effect as if such provision had not originally been contained in the MSA. 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.

14. The Agreement is governed by and constructed under Polish law.

15. Any dispute in connection to the Agreement shall be subject to the exclusive jurisdiction of the courts having jurisdiction over SALESmanago registered office.

16. Appendices shall form an integral part of the MSA.

17. If a conflict occurs between this MSA, appendices to the MSA and the Order Form, unless otherwise specifically stated in these documents, the order of precedence shall be:
    a. Order Form
    b. Appendix No. 1 to the MSA
    c. Appendix No. 3 to the MSA
    d. Appendix No. 4 to the MSA
    e. MSA.

Appendix No. 1 to the MSA 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 and when the Entruster is a processor, the Entruster also declares that all requirements in relation with the data controller have been met.

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: users of the Entruster's websites who are clients or potential clients of the Entruster;
   b. the type of personal data: name and surname, e-mail address, telephone number, Contact ID, IP number, location information, online behavioural data of data subjects;
   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 to the Processor only lawfully collected personal data and confirms that obtained all needed consents for processing personal data and all other consents to obtaining which applies data protection provisions.
2. Following a written request by the Entruster, the Processor shall 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 covered by the request, within 14 days of receiving such a request. Before sending a request mentioned above, the Entruster has to make an effort to obtain on its own all the necessary information related to processing personal data, for example, using documents and correspondence between parties while negotiating and executing PDPA.
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 Entruster grants the Processor a general authorisation for further entrustment of personal data. The Processor shall publish on its website a current list of both existing and planned sub-processors. The Entruster is obligated to periodically review this list, and in the event of any objection to the engagement of a specific sub-processor, the Entruster may exercise its right to object to such sub-processing. The right to object may be exercised solely prior to the planned sub-processing of personal data.

8. The full list of sub-processors is available **here**.

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. The Processor may inform the data subject that her or his request has been sent to the Entruster. The Processor may restrict the processing of the data subject's personal data for the duration of the Entruster's response to the data subject's request, particularly when the request concerns an objection to the processing of personal data for direct marketing purposes.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:

   10.1. **[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:

   10.1.1. 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);

   10.1.2. 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:

   10.1.2.1. 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;

   10.1.2.2. the likely consequences of the personal data breach;

   10.1.2.3. 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.

   10.1.3. 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.

   10.2. **[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:

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

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

   10.2.3. 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.

11. 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 Entruster or 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.

12. When required for personal data security reasons, for the duration of the investigation or until the causes of the breach are eliminated, the Processor may restrict the processing of personal data whose security is or could potentially be compromised (e.g., temporarily turning off a particular service or blocking mailings to specific contacts).

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 10 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. Standard contractual clauses referred to in §6(2) 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"
   1. adequately securing personal data in accordance with this PDPA in the part of the information system administered by the Entruster (for example, in case of improper security of the user account by assigning too weak password by the Entruster or disclosure of this password by the Entruster);
   2. processing personal data without the required consents that should have been obtained by the Entruster, and for processing personal data on the basis of defectively obtained consents;
   3. for processing personal data in violation of the Agreement or applicable laws if such processing results from improper integration of the System by the Entruster;
   4. failing to meet specific requirements under sector regulations that the Entruster is subject to (e.g., NIS2 Directive, DORA) unless the Entruster has informed the Processor about these requirements before the execution of the Agreement or within 14 days after these requirements took effect, and the Processor declared that it will meet these requirements to the extent they apply to the Processor.

§8 Representatives of the Parties

For the purposes of implementing this PDPA, the Entrustera nd 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. Without prejudice to the other provisions of the PDPA, this PDPA shall remain in force for the entire duration of the processing of the Personal Data entrusted by the Entruster, regardless of the termination or expiry of the Agreement.
3. In the event of terminating the Agreement, the Entruster shall, within 13 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,except for Personal Data processed as part of backups. Backups shall be created, in particular, to safeguard the data and ensure its availability during the Main Agreement's performance. The backups shall be stored for a maximum period of 12 months from their creation and automatically deleted after this period. The personal data stored in the backups are 'excluded from processing', which means that their processing is restricted to storage in encrypted form only, except if it becomes necessary to use the backup copy in connection with the performance of the Agreement, in accordance with the purpose of the backup copy, for example as a result of a failure of the system in which the data are processed during the performance of the Agreement. Only authorised persons acting on behalf of the Processor shall have access to such data. Concerning the backups, this Agreement shall be terminated upon the expiry of the storage period of the backups referred to above.
4. The Parties declare that any previously signed agreements regarding the processing of personal data are revoked and replaced by this PDPA.
5. Any issues falling outside the scope of this PDPA shall be governed by the provisions of the GDPR.

Appendix No. 2 to the MSA 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, address: ul. Klimeckiego 4, 30-705 Cracow, entered in the Register of Entrepreneurs of the National Court Register kept by XI Commercial

Division of the National Court Register of the District Court for Kraków-Śródmieście in Kraków under KRS number 0000523346, and NIP 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:	Data Protection Officer:
Benhauer sp. z o.o. based in Cracow	e-mail: dpo@salesmanago.com
Stanisława Klimeckiego 4	
30-705 Kraków	
e-mail: rodo@salesmanago.com	

Appendix No. 3 to the MSA - Terms of Onboarding Services

These Terms of Onboarding Services ("Terms") govern Customer's acquisition of SALESmanago Onboarding Services. Capitalized terms have the definitions set in the MSA unless expressly stated otherwise below.

§ 1 Subject matter of the Terms

1. SALESmanago agrees to provide to the Customer the Onboarding Services in accordance with the onboarding package selected by the Customer, as indicated in the Order Form. The scope of Onboarding Services is derived from the licence package selected by the Customer unless the Parties agree otherwise.
2. *usunięto*
3. The MSA shall apply to these Terms to the extent not covered by these Terms, unless expressly stated otherwise.
4. In the event of any discrepancy between the provisions of the MSA and these Terms, these Terms shall prevail.
5. Onboarding services are billed on the basis of Service Units (SU), the number of which is specified in the Order Form.

§ 2 Project scope and objectives

1. Notwithstanding anything to the contrary, the Parties acknowledge and agree that the Onboarding Services provided hereunder are limited in scope to the following. SALESmanago and Customer jointly agree there shall be no customizations to System's standard features and functionalities.
2. SALESmanago and the Customer shall work together to achieve the agreed-upon objectives below, according to the selected Onboarding Service package. Depending on the licence package selected by the Customer, the Onboarding Services will include the basic use cases described here[3].
3. By mutual agreement between the Parties, the Customer may use the purchased Service Units to carry out, in part instead of the base use cases, other use cases as indicated in the tables above.
4. The costs of the individual activities of the Onboarding Services expressed in SU and the scope of implementation are described here. For non-standard or complex implementations, the number of Service Units required may vary from the estimates provided here.

§ 3 Project assumptions and considerations

1. It is estimated that the chosen Onboarding Services will be completed within the time indicated in the Order Form starting from the Agreement start date according to the Order Form. If the Onboarding Services (or any part thereof) provided are not complete at the end of the above mentioned period due to Customer's failure to make the necessary resources (e.g. data which should be imported into the System) available to SALESmanago or to perform other Customer obligations in timely manner (e.g. unavailability of contact persons, failure to implement System integration), such Onboarding Services will be deemed to be complete at the end of the above mentioned delivery period.
2. All services shall be delivered remotely. Travel and related expenses shall not be required, and are not included in the fixed fee amount. No other fees and/or expenses will be permitted without the prior written approval of the Customer and SALESmanago.
3. SALESmanago may choose to change any personnel assigned to the Onboarding Services at any time for any or no reason.
4. The Customer will provide:
   a. appropriately qualified personnel, knowledgeable regarding the existing Customer's environment to support SALESmanago's activities in terms of the Onboarding Services. These personnel will be available without undue delay to clarify the business requirements and for validation of results as needed.
   b. ongoing access to the software required for this effort (e.g. plug-ins, if applicable);
   c. reasonably quick and expeditious resolution for business or technical questions or issues arising from the effort;
   d. that any data transferred to SALESmanago will be password protected and that the size of any file transferred will not exceed 20 MB
   e. Website integration, product feed, database, graphic design and materials, content, strategic guidelines.

---

[3] https://www.salesmanago.com/marketing-automation/use-cases.htm

5. The Customer undertakes to perform full System integration (monitoring code, transaction events submission, submission and contact monitoring, contact consent and subscription management, XML or product API configuration).
6. The Customer undertakes to inform about a possible change of the persons referred to in point 5a well in advance.
7. The Onboarding Services are limited only to the services related to the System. SALESmanago will not provide the content and will not configure external platforms.

§ 4 Fees and payments

1. The Customer will be charged a fixed fee for the Onboarding Services under the price list described in the Order Form.
2. The terms of payment for the Onboarding Services are described in the Order Form. Invoice for the Onboarding Services will be issued on Agreement start date, according to the Order Form (upfront payments).
3. Failure to make timely payment may result in the initiation of bad debt collection proceedings, the imposition of interest for late payment or withholding the provision of Onboarding Services.
4. Unknown circumstances may cause actual cost and effort to vary from the fees and timing outlined in these Terms and the Order Form. Any services beyond those described above will be subject to separate pricing.
5. Onboarding Services are non-cancellable, and all fees for Onboarding Services are non-refundable.

§ 5 Liability

1. In no event shall the aggregate liability of SALESmanago arising out of or related to the Onboarding Services exceed the total amount paid by Customer hereunder for the Onboarding Services. In no event will SALESmanago have any liability arising out of or related to the Onboarding Services 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.
2. Any limitation or modification which SALESmanago is entitled to make under these Terms shall not affect the assessment of the SALESmanago's due performance under these Terms and does not affect the remuneration payable to SALESmanago under these Terms.
3. The services provided under these Terms constitute a separate obligation from the remaining provisions of the Agreement. Therefore, SALESmanago's performance under these Terms shall not affect: (i) the assessment of the SALESmanago's due performance of the remaining obligations of the Agreement, nor shall it affect the validity of the Agreement or constitute a breach thereof in any other respect; (ii) the remuneration payable to SALESmanago under remaining part of the Agreement.

§ 6 Miscellaneous

1. The Terms apply only to the services indicated therein and do not regulate any Customer support after SALESmanago has completed their provision within the meaning of these Terms.
2. Termination of the provision of services under these Terms does not affect the validity and scope of the agreement regarding the use of the System.

Appendix No. 4 to the MSA
Information on jurisdiction

Information on jurisdiction

In accordance with Article 28(1)(a) of Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), the ICT infrastructure used for data processing within individual SALESmanago services is subject to the jurisdiction of the common courts in the Republic of Poland. To the extent that the ICT infrastructure used for data processing within individual SALESmanago services is operated by Google Cloud Poland sp. z o.o., it is subject to the jurisdiction of the London Court of International

Arbitration (LCIA) in London, United Kingdom. This excludes any necessary judicial interim measures, including, in particular, emergency, interim or injunctive relief, aimed at protecting the rights and interests of a party, which remain subject to general rules of jurisdiction.

Appendix No. 5
Exhaustive specification of all categories of data and digital assets that can be ported during the switching process, including, at a minimum, all exportable data

Exhaustive specification of exportable data categories and digital assets

SALESmanago provides a comprehensive capability to export customers' personal and non-personal data, covering the following categories: end-user, marketing, operational, and analytical data. This data is stored in the DC Play and Google Cloud Platform (GCP) infrastructure.

The company offers a wide selection of standard export formats: CSV (default export format from the user interface), JSON (default API format), and XLSX (alternative export format available from the application interface).

Personal data is processed in accordance with the data processing agreement. This includes, among others: first and last name, email, phone number, Contact ID, IP address, location, and online behavioral data, which can be classified as basic contact data, location data, purchasing preferences, and behavioral data.

Also exportable are digital assets, such as standard and custom reports, integration scripts used for automating marketing processes and integrating with external systems (e.g., CRM, ERP, e-commerce), as well as configuration files for customer segmentation, campaigns, and automation.

Additionally, SALESmanago offers the option to export data and resources beyond the standard scope available from the application. Such extended or custom exports are carried out based on individual pricing, tailored to the specific requirements of the client and the scope of the data.

Data / asset category	Location	Export format	Export method	Comment
Customer contact data	DC Play	CSV, JSON, XLSX	UI/API	Personal and contact data of customers.
Marketing campaign data	DC Play	CSV, JSON	UI/API	Campaign details, recipient segments.
Analytical reports	DC Play	CSV, JSON, XLSX	UI/API	Standard and custom reports.

Integration scripts	DC Play/GCP	JSON, source code	UI/Client's repository	External integrations (CRM, ERP, etc.)
Configuration files (segments, automations, campaigns)	DC Play/GCP	JSON/CSV	UI/API	Definitions of segments, automations, and campaigns.

Appendix No. 6

Exhaustive specification of categories of data specific to the internal functioning of the provider's data processing service that are to be exempted from the exportable data under Appendix No. 5, where a risk of breach of trade secrets of the provider exists, provided that such exemptions do not impede or delay the switching process

Exhaustive specification of data categories specific to the internal functioning of the data processing service provider, which are excluded from the exportable data

As a provider of a comprehensive Marketing Automation and Customer Data Platform (CDP), SALESmanago understands the key importance of providing our clients with full control over their data and the freedom to choose a service provider. In accordance with the requirements of the Data Act, we make every effort to ensure the data export process is transparent, effective, and uninterrupted.

At the same time, to protect our innovations and competitive advantage, it is necessary to precisely define those categories of data which, constituting the exclusive intellectual property and trade secret of SALESmanago, are excluded from the export mechanism. Below, we present a detailed specification of these categories, while guaranteeing that their exclusion will in no way hinder or delay our clients' process of switching providers, and that all data necessary to continue their operations will remain fully exportable.

Data / asset category	Example of data / assets	Justification
Data concerning the internal system architecture and infrastructure	Detailed database schemas, network diagrams, server configurations, data routing algorithms, hardware and software specifications used internally to provide the service, including application code.	Disclosure of this information could give SALESmanago's market competitors access to key know-how concerning the platform's optimization, scalability, and security, constituting a competitive advantage. Additionally, it could also create potential security vulnerabilities.
Unique algorithms and data models (including proprietary implementations of existing ones)	All AI/ML algorithms, predictive models, data compression algorithms, data transmission algorithms, resource optimization algorithms (e.g., allocation of virtual machines) that have been created by and are the intellectual property of the provider. This also applies to database schemas	The algorithms and data models developed by SALESmanago are the result of years of research and development, which constitute our technological advantage and service efficiency. Disclosure of this information could allow SALESmanago's market competitors to copy these

	designed internally for storing and processing data in a unique, optimized way.	solutions without incurring the costs of their development.
Internal performance monitoring and management tools	Specific tools and methodologies used for internal monitoring of our systems' performance, anomaly detection, load management, problem-solving, and resource optimization.	These tools are an integral part of the organization's ability to maintain high availability and performance of services. Their specifics and mode of operation constitute valuable operational knowledge.
Data concerning internal operational and security processes	Detailed incident response procedures, internal security audits, specific internal authentication and authorization protocols, business continuity and disaster recovery plans (unless they directly concern client data).	Data in this category is classified as critical for maintaining the security and reliability of the services provided. Disclosure of this information could create security vulnerabilities or enable sabotage.

Appendix No. 7

Information on available procedures for switching and porting to the data processing service, including information on available switching and porting methods and formats as well as restrictions and technical limitations which are known to the provider of data processing services

Procedures for switching data processing service providers

SALESmanago enables the free migration of client data to other service providers through simple and effective export mechanisms. Users can export data and resources through both the application interface (UI) and via API, in popular formats such as CSV, JSON, and XLSX. SALESmanago monitors technical export limits, such as single export file size restrictions and an API request limit of 500 requests per minute, to ensure optimal infrastructure performance.

Migration procedure / method	Availability	Technical limitations	Comments / notes
Data export via UI	YES	Maximum export file size	CSV/XLSX export
Data export via API (JSON)	YES	API request limit/minute	Client integration required
Migration between other providers	NO	-	Not possible due to costs

Appendix No. 8

Up-to-date online register hosted by SALESmanago, with details of all the data structures and data formats as well as the relevant standards and open interoperability specifications, in which the exportable data referred to in Appendix No. 5, are available.

Register of data structures, formats, and interoperability standards for exportable data

In accordance with interoperability requirements, SALESmanago provides a public register of technical information for exportable data that can be transferred when switching a data processing service provider. The register contains detailed information about:

- data structures used for export (e.g. contact, email, campaign),

- available formats (CSV, JSON, XLSX, source code),

- open standards and technical specifications used to ensure interoperability,

- validation standards used in the SALESmanago API (in accordance with v3/v2 documentation).

By using commonly accepted formats (RFC, ISO, JSON Schema, OpenAPI), the data can be reused in CRM, ERP, marketing automation, or BI systems.

Data / asset category	Export format	Interoperability standards and specifications
Customer contact data	CSV, JSON, XLSX	- RFC 882 (Email) - ietf.org - RFC 4122 (UUID) - ietf.org - ISO 8601 (dates) - iso.org - ISO 3166-1 (countries) - iso.org - RFC 4180 (CSV) - ietf.org
Marketing campaign data	JSON, CSV	- JSON Schema → json-schema.org - ISO 8601, UUID
Analytical reports	JSON, CSV, XLSX	- CSVW (CSV on the Web) → w3.org - ISO 8601, UUID
Integration scripts	JSON, source code	- OpenAPI 3.0 - JSON Schema
Configuration files (segments, automations, campaigns)	JSON, CSV	- JSON Schema - ISO 8601, UUID

Appendix No. 9

General description of the technical, organisational and contractual measures adopted by the provider of data processing services in order to prevent international governmental access to or transfer of non-personal data held in the Union where such access or transfer would create a conflict with Union law or the national law of the relevant Member State

General description of technical, organizational, and contractual measures adopted by the data processing service provider to prevent international government access or transfer of non-personal data stored in the Union

- General policy on the security of personal data and IT systems

- Procedures for reporting breaches

- Periodic reviews of internal procedures

- Procedure for handling abuse

- Data Protection Officer

- Issuance of authorizations for personal data processing

- Training in personal data protection

- Declarations of confidentiality regarding personal data

- Restriction of access to the personal data processing area (physical locations), particularly through access cards, access codes, locked cabinets and rooms, video surveillance, alarm systems, security services, and restricted access to IT systems and networks (using logins, passwords, separate networks for third parties, and automatic screen locks).

- Procedure for granting and revoking access rights to IT systems

- Password policy

- Use of secure network connections, e.g., VPN

- High Availability Cluster

- Measures to ensure event logging, e.g., Microsoft Clarity, Internal logging system

- Anti-DDoS system, e.g., WanGuard

- Conducting quarterly vulnerability tests of IT systems

- Conducting penetration tests of IT systems

- Antivirus software

- Cybersecurity training

- Procedure for verifying service providers for regulatory compliance and adequate security measures

- Cyclical risk analysis of the violation of rights and freedoms of individuals whose data is processed

- Security and privacy risk analysis carried out at least once a year

- Procedures for applying the privacy by design principle in software development

- Standard for maintaining the privacy by default principle in the design phase

- Use of cryptographic measures for personal data protection, e.g., SSL protocol [TLS 1.2 - 1.3 + SHA256]

- Securing data transmission with the HTTPS protocol

- Use of multi-factor user authentication in the ICT system

- User identification and authorization measures, e.g., Basic Auth login panel

- Audit logs for mass data modification actions on the platform

- Individual login indicators

- Personal Data Processing Agreement, including a contractual prohibition on transferring personal data outside the European Economic Area without the controller's consent [89]

- Confidentiality Agreement

Appendix No. 10
Information on data processing services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets or service architecture.

Information on services whose migration is particularly difficult or costly

The current architecture of the SALESmanago system does not have significant technical or organizational limitations that would hinder migration to another service provider. All client data is fully exportable through the available UI and API mechanisms. There are no complex technological dependencies that could prevent or significantly hinder such a migration. The company uses open standards and popular export formats, thereby minimizing the risk of vendor lock-in.

Component / service	Migration difficulty	Export capabilities	Notes
Customer data	Easy	CSV, JSON, XLSX	Export available via UI/API
Reports and campaign configurations	Easy	CSV, JSON	Export available via UI/API
External integrations	Medium	JSON, source code	Reconfiguration of integrations required on the new provider's side
Specific technological dependencies	None	-	No known technological limitations