MAIN SERVICES AGREEMENT

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

By accepting this Main Services Agreement, 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**" – an account enabling the use of the Services, understood as the use of a selected package.
2. "**Agreement**" means agreement concluded between the Customer and SALESmanago on the basis of the Order Form and the MSA.
3. **"Confidential Information"** – 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.
4. "**Customer**" means the individual, a company or other legal entity which has entered into Order Forms.
5. **"GDPR"** – 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).
6. "**MSA**" means this Main Services Agreement.
7. "**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.
8. "**Parties**" – Customer and SALESmanago.
9. "**Password**" - a sequence of signs, including alphanumeric, necessary to perform an authentication process while accessing the Account, determined by the User during the registration process.
10. "**Personal Data Protection Regulations**" - regulations regarding processing of Personal Data including GDPR and The Personal Data Protection Act.
11. "**Personal Data**" - means any information relating to an identified or identifiable natural person according to the Personal Data Protection Regulations.
12. "**SALESmanago**" means Benhauer sp. z o. o. based in Cracow (31-532) at Grzegórzecka 21, NIP: 676 244 77 54 REGON: 122334666, entered into the Register of Entrepreneurs kept by the District Court for Kraków Śródmieście in Kraków, Division XI of the National Court Register under entry number KRS: 0000523346, with a share capital in the amount of PLN 1 407 450.00.
13. "**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.
14. "**System**" – online Customer Engagement Platform.
15. "**The Personal Data Protection Act**" – The Act of 10 May 2018 on the Protection of Personal Data (Dz.U. 2019.1781 t.j. with subsequent amendments).
16. **"Third Party Provider"** - a provider of Third Party Services.
17. **"Third Party Services"** - services provided by a Third Party Provider to Customer in connection with the use of the System.

18. “**User profile**” - 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.
19. “**User**” - a natural person above 18 years of age 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 behavioral and transactional data about the Customer’s clients and delivers personalised communications across all marketing channels.
2. During the period and to the extent specified in the Order Form, SALESmanago will provide support performed by a dedicated SALESmanago Specialist ("Onboarding”), which includes:
    a. Configuration of User’s Accounts and email accounts for email marketing purposes;
    b. Preparation and implementation of a newsletter template based on the design delivered by the Customer;
    c. Import of email contacts database provided by the Customer and execute email marketing campaigns;
    d. Implementation of automatic contacts database segmentation and configuration of basic marketing automation scenarios.

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 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 and agents who need such access for the purpose of the Agreement. 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.
3. The Customer is obliged to use the System in compliance with the rules of law and in good faith.
4. While using the Services, the Customer is obliged, in particular to:
    a. use the System in a way that does not distort their 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;
    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.
6. The minimum technical requirements which enable using 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.com and/or salesmanago.pl websites.
    b. Services available through salesmanago.com website (admin panel): access to the internet, the latest version of one of the following web browsers: Google Chrome, Microsoft Edge, Mozilla Firefox with a default configuration.
7. The Customer may choose to obtain Third Party Services (e.g. applications) to use with features within the System. To use such features, the Customer will be required to obtain access to Third Party Services from Third Party Providers. Any acquisition by Customer of Third Party Services, any exchange of data between Customer and Third Party Providers, and governing terms are solely between Customer and the applicable Third Party Provider. SALESmanago assumes no responsibility for, and specifically disclaims any liability, warranty, and obligation with respect to Third Party Services, whether or not it is recommended or approved by SALESmanago, or otherwise noted.

V. FEE AND PAYMENTS

1. The Customer will be charged a monthly fee for the Services under the detailed price list described 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 a settlement period.
3. Fees indicated in the Order Form will be increased by the indicated value on each renewal as an Annual Innovation Premium. The indicated fee increase does not require an amendment to the Agreement.
4. If during the term of the Agreement the Customer reaches a given threshold of the number of 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 stored in the System database.

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 organized 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. 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.

VIII. MISCELLANEOUS

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 7 days from receiving the notification from the Customer.
3. 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,
    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**,
    c. breach by the Customer of the rules of law.
4. 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.

5. 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.
6. SALESmanago may at any time make any change to any Service that is necessary to comply with applicable law, or that does not materially affect the nature or quality of the Service.
7. According to the Personal Data Protection Regulations, Parties have regulated the principles of entrusting the processing of Personal Data, in the agreement constituting Attachment No. 1 to the MSA.
8. Information on the processing by SALESmanago of personal data of Customer's representatives and persons responsible for the coordination and implementation of the Agreement constituting Attachment No. 2 to the MSA. The Customer undertakes to provide this information to the data subjects.
9. Any amendment or variation to this 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.
10. 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.
11. The Agreement is governed by and constructed under Polish law.
12. Any dispute in connection to the Agreement shall be subject to the exclusive jurisdiction of the courts of Kraków, Poland.
13. Attachments shall form an integral part of the MSA.

Attachment No. 1 to the MSA Personal Data Processing Agreement

Personal Data Processing Agreement

hereinafter referred to as „PDPA”

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

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

§ 1 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 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), hereinafter referred to as the ‘GDPR’ as well as the proper performance of the Agreement, the Controller, 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 Controller and the Processor provides sufficient guarantees to implement appropriate technical and organizational 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.

§ 2 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 Controller's websites who are clients or potential clients of the Controller;
   b. the type of personal data: name and surname, e-mail address, telephone number, Contact ID, IP number, online behavioral 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 databases and Internet service in the duration of the same term as the performance of the Agreement.
2. The Processor undertakes to process entrusted personal data only for the purpose and scope specified in above, based on documented instructions from the Controller, which also applies to the transfer of personal data to a third country or international organization (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 Controller 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).

§ 3 Rights and obligations of Parties

1. The Controller entrusts to the Processor lawfully collected personal data.
2. Following a written request by the Controller, 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.
3. The Processor shall inform the Controller 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 organization, in accordance with Article 28(3) point a of the GDPR.
4. The Processor ensures that persons authorized 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 Controller 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.
8. The Processor takes into account the nature of the processing, assists the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller'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 not obliged to respond directly to the requests of the data subjects.
9. The Processor assists the Controller 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:
    9.1. **[Data breach concerning data processed by the Controller]** In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:
        9.1.1. in notifying the personal data breach to the competent supervisory authority, without undue delay after the controller 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);
        9.1.2. in obtaining the following information which, pursuant to Article 33(3) of the GDPR, shall be stated in the Controller's notification, and should include:
            9.1.2.1. 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;
            9.1.2.2. the likely consequences of the personal data breach;
            9.1.2.3. the measures taken or proposed to be taken by the Controller 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.

        9.1.3. 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.
    9.2. **[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 controller without undue delay but no later than 24 hours after the Processor having become aware of the breach. Such notification shall contain:
        9.2.1. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
        9.2.2. the details of a contact point where more information concerning the personal data breach can be obtained;
        9.2.3. 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.

10. The Processor makes available to the Controller 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 Controller or another auditor mandated by the Controller, in accordance with Article 28(3) point h of the GDPR and under the conditions set out in §4 below.

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

§4 Audits

1. The Controller 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 Controller 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 Controller's questions, insofar as this is possible, within 30 days of receiving them.
3. After the audit referred to in point 2 above, the Controller, 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 Controller's request), its exact scope, and persons authorized 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 Controller undertakes to keep the above-mentioned information confidential. Before starting the audit activities, the Parties (and an external auditor appointed by the Controller, if applicable) will sign an appropriate confidentiality agreement.
5. The costs of the audit are borne by the Controller.

§5 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. 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 Controller. 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 Controller 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.
3. 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 Controller.

§6 Representatives of the Parties

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

a. The Controller: contact person indicated in the Order Form
b. The Processor:
   Name: Piotr Uryga, email: piotr.uryga@salesmanago.com
   - the indicated person may be changed at any time via email. Such change does not constitute an amendment to the PDPA.

§7 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 Controller 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 in accordance with Article 28(3) point g of the GDPR.
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.

Attachment No. 2 to the MSA Information on the processing of personal data for the Customer, persons representing the Customer, Users and contact persons

Who will process personal data and how to contact them

1. **Benhauer sp. z o. o.** based in Cracow (31-532) at Grzegórzecka 21, KRS number: 0000523346 (the "**Company**") is the controller of the personal data, within the meaning of Regulation (EU) No. 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) (the "**GDPR**"), of the Contractor who is a natural person, Representatives and Contact Persons.
2. Requests, declarations and all correspondence regarding personal data should be sent in writing or by e-mail to the Company's addresses indicated in point 1 or 3.
3. Please be advised that we have appointed a data protection officer, who can be contacted at: piotr.uryga@salesmanago.com. You can contact the data protection officer in all matters relating to the processing of personal data and the exercise of rights related to data processing.

Definitions

4. **Contractor** - a natural person running a business or a legal person or other organizational unit with which the Company enters into business cooperation.
5. **Representative** - a representative or proxy of the Contractor with whom the Company has concluded an agreement in order to cooperate with the Company.
6. **Contact Person** - any natural person who contacts employees and representatives or proxies of the Company in order to establish or implement business cooperation and the User, in particular, the contact person may be an employee of the Contractor or another person appointed by the Contractor, or acting on its behalf.

Who was the data obtained from?

7. If you are the Representative, personal data has been obtained directly from you, as a representative of the Contractor, under the agreement between the Contractor and the Company (the **"Agreement").**
8. If you are a Contact Person, personal data has been obtained directly from you or from a Contractor as part of the cooperation with the Company.

Scope of processed data

9. The scope of processed data includes the following categories:
    a) identification data (e.g. name and surname, tax identification number, place of work, position held),
    b) contact details (e.g. telephone number, e-mail address),
    c) in the case of Users of the SALESmanago system also data on activity within the system, login data,
    d) other data provided by the Contractor or provided directly by you in connection with the conclusion or performance of the Agreement.

Purposes and legal grounds for the processing of personal data

10. Your personal data will be processed for the following purposes:
    a) conclusion and performance of the Agreement - the legal basis for the processing of the Contractor's data who is a natural person is the necessity of processing to perform the Contract or to take steps at the request of the Contractor prior to entering into a Contract (Article 6 (1) (b) of the GDPR);
    b) enabling the performance of the Agreement, including verification whether the person who contacts the Company is authorized to act on behalf of the Contractor - the legal basis for processing the data of the Contact Person and the Representative is the legitimate interest of the Company (Article 6 (1) (f) GDPR);
    c) compliance with obligations under the law, including in particular tax and accounting regulations - the legal basis for the processing of the data of the Contractor who is a natural person, Representative and Contact Person is the legal obligation (Article 6 (1) (c) of the GDPR);
    d) managing relations with the Contractor - the legal basis for processing the data of a Contractor who is a natural person, Contact Person and Representative is the legitimate interest of the Company (Article 6 (1) (f) of the GDPR);
    e) conducting direct marketing of the Company's products and services - the legal basis for the processing of the data of the Contractor who is a natural person, the Contact Person and the Representative is the legitimate interest of the Company (Article 6 (1) (f) of the GDPR);
    f) Contractor's satisfaction surveys regarding the Company's products and services - the legal basis for processing the data of a Contractor who is a natural person, Contact Person and Representative is the legitimate interest of the Company (Article 6 (1) (f) of the GDPR);
    g) ensuring the safety of the Company's employees / coworkers or the protection of property or secrecy of information, the disclosure of which could expose the Company to damage - the legal basis for processing the data of the Contractor who is a natural person, Representative and Contact Person is the legitimate interest of the Company (Article 6 (1) (f) of the GDPR);
    h) establishing or pursuing possible claims or defending against such claims by the Company - the legal basis for processing the data of the Contractor who is a natural person, Representative and Contact Person is the legitimate interest of the Company (Article 6 (1) (f) of the GDPR in conjunction with Article 9 (2) (f) of the GDPR);
    i) archival (evidence) which are the implementation of the legitimate interest of the Company in securing information in the event of a legal need to prove facts - the legal basis for processing the data of the Contractor who is a natural person, Representative and Contact Person is the legitimate interest of the Company (Article 6 (1) (f) of the GDPR in conjunction with Article 9 (2) (f) of the GDPR);
    j) the purposes indicated each time in the consent clause, the expression of which may be requested by the Company - the basis for processing the data of the Contractor who is a natural person, Representative and Contact Person is the consent of the data subject (Article 6 (1) (a) of the GDPR).

Is the provision of personal data obligatory?

11. If personal data is processed in connection with the conclusion of the Agreement and its performance, providing the data is voluntary, but without providing it, it is not possible to conclude the Agreement and take action in connection with its implementation.
12. If the processing of personal data is necessary to fulfill the legal obligation incumbent on the Company, the provision of personal data is a statutory requirement.
13. If personal data are processed for purposes resulting from legitimate interests pursued by the Company or by a third party, the provision of personal data is voluntary, but necessary to achieve these purposes.
14. If personal data are processed on the basis of the consent of the data subject, the provision of personal data is voluntary. Failure to provide data will result in the inability to achieve a given goal, if consent is a condition for achieving this goal.

Who will the personal data be transferred to?

15. Your personal data may be transferred only if it is justified by the pursued purpose, to the following categories of recipients: entities providing services to the Company, such as accounting and tax services, auditing, postal operators and couriers, IT system suppliers and IT services, insurers, entities providing technical, organizational and advisory support, entities providing legal services, entities providing archiving services, entities providing debt collection services, entities authorized under the law, entities related by shares or personally with the Company.

How long will personal data be processed?

16. The period of storage of your personal data depends on the purpose for which the data is or may be processed.
17. In the case of data processing in connection with the conclusion and performance of the Agreement, personal data will be processed for the duration of the Agreement, and after its termination for the period necessary to perform obligations or rights under the law and the period of limitation of claims and until the completion of civil proceedings, enforcement, administrative and criminal proceedings requiring data processing.
18. If the processing is necessary to fulfill the legal obligation incumbent on the Company, personal data will be processed for the period resulting from the generally applicable provisions of law (in particular the provisions of tax and accounting law).
19. In the case of data processing for the purpose of managing the relationship with the Contractor - personal data will be processed for the duration of this relationship.
20. In the scope of data processing by the Company for the purpose of direct marketing, personal data will be processed for the period of maintaining the relationship with the Contractor or until an objection to the processing of your personal data for this purpose is raised.
21. In the scope of data processing for purposes other than the above-mentioned based on the premise of the legitimate interest of the Company, personal data will be processed for a period not longer than it is necessary to achieve these purposes.
22. In the scope of data processing on the basis of consent to data processing for specific purposes - personal data will be processed until the consent is withdrawn or until the purpose covered by the consent statement is achieved.

What rights do you have regarding your personal data?

23. You have the right to: access data, rectify data, erase data, restrict its processing and the right to data portability (if the processing is based on consent or a contract in an automated manner).
24. You have the right to object to the processing of data for purposes carried out on the basis of the legitimate interest of the Company on grounds relating to your particular situation. We will no longer process your data for these purposes, unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims. You also have the right to object to the processing of data for direct marketing purposes.
25. To the extent that the basis for the processing of your personal data is consent, you have the right to withdraw your consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
26. The above requests and declarations should be submitted in the manner indicated in point 2 above.

Where can I file a complaint regarding the processing of personal data?

27. If you believe that the processing of your personal data violates the law, you may submit a complaint to the supervisory body dealing with the protection of personal data. In the Republic of Poland, the supervisory body is the President of the Personal Data Protection Office.