

Appendices to the Main Services Agreement

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

Manago AI, 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;

ver. 6.0.

- 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.

ver. 6.0.

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;

ver. 6.0.

- 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](#).

ver. 6.0.

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@manago.ai.
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 Entruster and the Processor appoint a contact person:

- a. The Entruster: contact person indicated in the Order Form
- b. The Processor: email: dpo@manago.ai
 - 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.

ver. 6.0.

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.

ver. 6.0.

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

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

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

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

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

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

The data controller:
Benhauer sp. z o.o. based in Cracow
Stanisława Klimeckiego 4
30-705 Kraków
e-mail: rodo@manago.ai

Data Protection Officer:
e-mail: dpo@manago.ai

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

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

§ 1 Subject matter of the Terms

1. Manago AI 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.

ver. 6.0.

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. Manago AI and Customer jointly agree there shall be no customizations to System's standard features and functionalities.
2. Manago AI 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](#)¹.
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 Manago AI 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 Manago AI.
3. Manago AI 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 Manago AI'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 Manago AI 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.

¹ <https://manago.ai/use-cases>

ver. 6.0.

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. Manago AI 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 Manago AI 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 Manago AI 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 Manago AI is entitled to make under these Terms shall not affect the assessment of the Manago AI's due performance under these Terms and does not affect the remuneration payable to Manago AI under these Terms.
3. The services provided under these Terms constitute a separate obligation from the remaining provisions of the Agreement. Therefore, Manago AI's performance under these Terms shall not affect: (i) the assessment of the Manago AI'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 Manago AI 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 Manago AI 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

ver. 6.0.

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 Manago AI 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 Manago AI 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

Manago AI 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, Manago AI 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
-----------------------	----------	---------------	---------------	---------

ver. 6.0.

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), Manago AI 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 Manago AI, 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
-----------------------	--------------------------	---------------

ver. 6.0.

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 Manago AI'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 designed internally for storing and processing data in a unique, optimized way.	The algorithms and data models developed by Manago AI are the result of years of research and development, which constitute our technological advantage and service efficiency. Disclosure of this information could allow Manago AI's market competitors to copy these 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

ver. 6.0.

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

Manago AI 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. Manago AI 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 Manago AI, 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, Manago AI 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 Manago AI API (in accordance with v3/v2 documentation).

ver. 6.0.

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

ver. 6.0.

- 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

ver. 6.0.

- 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 Manago AI 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