

REGULATIONS FOR ENTRUSTING THE PROCESSING OF PERSONAL DATA

§ 1.

Subject of the Regulations

1. The subject matter of the Regulations is to describe the principles of entrusting the processing of personal data, pursuant to Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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) (OJ EU L of May 4, 2016, hereinafter: GDPR), in connection with the use of the Reservation System.
2. Prior to entering into an Entrustment Agreement, the Personal Data Controller is required to read and accept the Regulations. The Entrustment Agreement shall be concluded upon acceptance of the Regulations by the Personal Data Controller.

§ 2.

Definitions

The terms used in the Regulations mean the following:

1. **Personal Data Controller** — a "Personal Data Controller" shall mean an individual, legal entity, or organizational unit with legal capacity that uses the Reservation System and enters into the Prime Agreement with the Processor for this purpose;
2. **audit** — an "audit" shall mean an independent audit of the processing of personal data at the Processor's organization, aimed at confirming that the processing of personal data by the Processor is carried out in accordance with the Regulations and the applicable personal data protection regulations, in particular Regulation 2016/679;
3. **auditor** — an "auditor" shall mean an independent entity professionally engaged in conducting audits in the field of personal data, authorized by the Personal Data Controller to conduct an audit on their behalf, the selection of which shall be agreed upon each time and made by the Personal Data Controller jointly and in consultation with the Processor, provided, however, that the auditor shall not be an entity that conducts business competitive to the Processor (or their affiliates) or is affiliated, directly or indirectly, with any entity that conducts business competitive to the Processor (or their affiliates);
4. **personal data** — "personal data" shall mean any information about an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular on the basis of an identifier such as a name and surname, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the natural person;
5. **personal data breach** — a "personal data breach" is defined as a breach of security leading to the accidental or unlawful destruction, loss, modification, unauthorized disclosure of, or unauthorized access to personal data transmitted, stored, or otherwise processed;
6. **data subject** — a "data subject" shall mean an individual whose personal data have been entrusted to the Processor for processing;
7. **Processor** — the term "Processor" shall mean MPR Spółka z ograniczoną odpowiedzialnością with its registered office in Warsaw, 6 Floriańska Street, premises 02, 03-707 Warsaw, entered in the National Court Register by the District Court for the Capital City of Warsaw in Warsaw, XII Economic Division of the National Court Register, under KRS number: 0000788188, TIN number: PL5783137225, share capital: PLN 10,000;
8. **processing of personal data** — "processing of personal data" shall mean an operation or set of operations performed on personal data or sets of personal data in an automated or non-automated manner, such as collecting, recording, organizing, structuring, storing, adapting or modifying, downloading, viewing, using, disclosing by transmitting, distributing or otherwise making available, adjusting or linking, limiting, erasing, or destroying;
9. **Parties** — by "Parties" is meant the Personal Data Controller and the Processor;

10. **Reservation System** — by "Reservation System" is meant the ICT system named "Calendesk" belonging to the Processor, which is available at the electronic address <https://calendesk.com/> and under which the Processor provides ICT resources to the Personal Data Controller;
11. **means of electronic communication** — "means of electronic communication" should be understood as technical solutions, including ICT devices and software tools cooperating with them, enabling individual communication at a distance using data transmission between ICT systems, and in particular electronic mail;
12. **Entrustment Agreement** — the "Entrustment Agreement" shall mean the agreement for entrustment of personal data processing concluded between the Personal Data Controller and the Processor pursuant to these Regulations;
13. **Prime Agreement** — the "Prime Agreement" shall mean the agreement for the provision of services related to the use of the Reservation System concluded between the Personal Data Controller and the Processor with respect to the basic legal relationship;
14. **Regulation 2016/679** — by "Regulation 2016/679" is meant Regulation 2016/679 of the European Parliament and of the Council (EU) of April 27, 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) (OJ EU L of May 4, 2016).

§ 3.

Entrustment of personal data processing

1. The Parties hereby declare that they have entered into the Prime Agreement, the execution of which entails entrusting the Processor with personal data for processing on behalf of the Personal Data Controller.
2. Pursuant to the Entrustment Agreement, the Personal Data Controller entrusts the Processor with personal data for processing, and the Processor undertakes to process the personal data under the terms of the Entrustment Agreement.
3. The Personal Data Controller declares that they will independently fulfill all information obligations to data subjects whose personal data have been entrusted to the Processor for processing.
4. The Processor declares that they have implemented appropriate technical and organizational measures to ensure that the processing of entrusted data meets the requirements of the Regulation and protects the rights of data subjects. The Processor undertakes to process the entrusted personal data in accordance with the Entrustment Agreement, Regulation 2016/679, and other generally applicable laws that protect the rights of data subjects.

§ 4.

Nature and purpose of processing

1. The nature of personal data processing results from the Prime Agreement, i.e. the processing of personal data by the Processor involves the processing of personal data in an automated and non-automated manner, in computer systems and outside computer systems (paper records), and will include such activities as recording, organizing, structuring, storing, modifying, viewing, using, transmitting, sharing, restricting processing, deleting, and destroying personal data.
2. The processing of personal data by the Processor, in accordance with the Prime Agreement, will be aimed at performing services related to making the Reservation System available for use by the Personal Data Controller. The entrustment of the processing of personal data is necessary for the performance of the duties provided for in the Prime Agreement.
3. The Processor shall not process the entrusted personal data for any purposes not agreed with the Personal Data Controller.

§ 5.

Types of entrusted personal data

1. The Personal Data Controller entrusts the Processor with the processing of the following categories of personal data:

- a. name and surname;
 - b. email address;
 - c. phone number;
 - d. image;
 - e. company;
 - f. tax identification number;
 - g. statistical identification number (REGON);
 - h. business address;
 - i. type of reservation;
 - j. date of reservation;
 - k. place of reservation;
 - l. reservation history;
 - m. information on passes and subscriptions;
 - n. information on discounts, rebates, etc;
 - o. IP address;
 - p. information about the case in which the customer is contacting;
 - q. data related to accepting payments with a third-party payment operator;
 - r. personnel position/function;
 - s. internal phone identification number for sending push notifications;
 - t. data related to the identification of the account and specific customer of the Personal Data Controller in the invoicing system;
 - u. Internet domain address;
 - v. content of notifications sent to customers / personnel;
 - w. information about the resources needed for the reservation, such as the number of rooms, the number of chairs, etc.
2. The Processor shall not, without the knowledge and consent of the Personal Data Controller, process on their behalf personal data other than those specified in paragraph 1.

§ 6.

Categories of personal data subjects

The Personal Data Controller entrusts the Processor with the processing of personal data concerning the following categories of data subjects:

- a. customers of the Personal Data Controller;
- b. users of the website;
- c. contact persons on the part of the customers of the Personal Data Controller;
- d. personnel of the Personal Data Controller.

§ 7.

Time of entrustment of personal data processing

1. The Personal Data Controller entrusts the Processor with the processing of personal data for the duration of the Prime Agreement.
2. The Entrustment Agreement shall be entered into for the term of the Prime Agreement and shall expire or terminate simultaneously upon expiration or termination of the Prime Agreement.
3. Upon the expiry or termination of the Agreement, the Processor is obliged to cease further processing of personal data on behalf of the Personal Data Controller. In the event of violation of this provision, they will be considered the controller of personal data with regard to personal data processed without the request of the Personal Data Controller.
4. Subject to paragraphs 5–7, upon expiration or termination of the Entrustment Agreement, the Processor is obliged, at the choice of the Personal Data Controller, to:
 - a. delete any existing copies of the personal data — within 14 (in words: fourteen) days from the date of receipt of the Personal Data Controller's request, at the latest, or

- b. return the entrusted personal data to the Personal Data Controller in the manner specified by the Personal Data Controller — no later than 14 (in words: fourteen) days from the date of receipt of the Personal Data Controller's request.
- 5. The Processor shall not be obliged to delete or return personal data when Polish or European law requires the Processor to continue to store personal data, regardless of the expiration or termination of the Entrustment Agreement.
- 6. The Processor shall not be obliged to delete or return personal data when further processing of the entrusted personal data is necessary for the purposes of the legitimate interests of the Processor, which shall be understood as, in particular:
 - a. the Processor's need to demonstrate that they have duly performed the Prime Agreement;
 - b. the establishment, redress, or defense against potential claims related to the performance of the Prime Agreement, including claims for tort damages — for the period of the statute of limitations for such potential claims, taking into account the additional period for activities related to such claims;
 - c. the purposes and obligations of the Processor under the relevant professional norms or standards for the Processor's activities;
 - d. the purposes and obligations of the Processor arising from the Processor's internal procedures and policies, including, in particular, those aimed at fulfilling requirements related to the protection of personal data.
- 7. In the event that the Processor continues to store personal data in accordance with paragraph 6 after the execution of the Prime Agreement, the Processor shall become an independent controller of personal data in this regard.
- 8. Upon request of the Personal Data Controller, the Processor shall confirm that all entrusted personal data have been permanently deleted or returned to the Personal Data Controller.

§ 8.

Responsibilities of the Personal Data Controller

Under the Entrustment Agreement, the Personal Data Controller is required to:

- a. ensure that all entrusted personal data are processed by them in accordance with the law, in particular with respect to the legal basis legalizing the processing of personal data;
- b. ensure that the entrustment of personal data processing is carried out in accordance with the requirements of Regulation 2016/679;
- c. cooperate with the Processor in the execution of the Entrustment Agreement;
- d. provide the Processor with all necessary explanations and information regarding the processing of personal data on their behalf;
- e. notify the Processor of all circumstances affecting the performance of the Entrustment Agreement;
- f. notify the Processor of any inspections conducted by state authorities, including the President of the Personal Data Protection Office, if the inspection is related to the Processor's activities;
- g. notify the Processor of any claims by data subjects related to the processing of personal data entrusted to the Processor;
- h. notify the Processor of the expiration of the stipulated period of processing of personal data and the need to delete or destroy such data, in accordance with the personal data retention procedure adopted by the Personal Data Controller. If the Personal Data Controller fails to instruct the Processor to delete or destroy the Personal Data, the Processor shall be obligated to retain such data until instructed to do so.

§ 9.

Responsibilities of the Processor

- 1. The Processor shall process personal data only upon the documented instruction of the Personal Data Controller and to the extent specified by the Personal Data Controller, subject to 2.

2. The Processor is authorized to process personal data if such obligation is imposed on them by European Union law or national law. In such a case, the Processor shall, prior to the processing of personal data, inform the Personal Data Controller of this legal obligation, unless such information is prohibited by law for reasons of important public interest.
3. The documented order of the Personal Data Controller referred to in paragraph 1 shall be considered to be each time an order to process personal data resulting from:
 - a. the subject matter of the Prime Agreement or the Entrustment Agreement;
 - b. a written document signed by a person authorized to represent the Personal Data Controller;
 - c. an email or text message sent by a person authorized to represent the Personal Data Controller.
4. The Processor shall ensure that all persons authorized by the Processor to process personal data are bound to secrecy or are subject to the relevant statutory obligation to ensure secrecy.
5. The Processor shall ensure that only authorized persons who are familiar with the principles of personal data protection and are properly trained in such matters have access to personal data.
6. The Processor shall maintain a register of all categories of processing activities, noting in it all information required by Article 30(2) of Regulation 2016/679, unless exempted from this obligation by law.
7. The Processor shall, to the extent possible, support the Personal Data Controller in fulfilling their obligations under Articles 32–36 of the GDPR.
8. If the Processor concludes that the order issued by the Personal Data Controller violates:
 - a. applicable data protection laws;
 - b. the Prime Agreement or the Entrustment Agreement;
 - c. the interests of the Processor,they shall immediately notify the Personal Data Controller, indicating which instruction and why, in their opinion, violates applicable laws, agreements, or interests.
9. In the cases referred to in paragraph 8, if the Personal Data Controller maintains the instruction despite the notification of objections, the Processor may:
 - a. refuse to carry out the order — without any negative consequences for breach of the Prime Agreement or the Entrustment Agreement, or
 - b. execute the order as requested by the Personal Data Controller — at the expense and risk of the Personal Data Controller.

§ 10.

Further entrustment of personal data processing

1. As a general rule, the Processor may use the services of a sub-processor by means of a written agreement under which the same obligations will be imposed on the sub-processor as on the Processor.
2. When subcontracting personal data to a third party for further processing, the Processor shall follow the principle of minimalism and provide such entities only with the data necessary for them to provide the specific services for which the personal data are subcontracted.
3. The Parties agree that the Processor may process personal data:
 - a. in a member state of the European Union;
 - b. in another country that is a signatory to the Agreement on the European Economic Area (EEA);
 - c. in another country recognized by the European Commission as a place ensuring an adequate level of personal data protection;
 - d. in a country other than those specified in point (c), with other mechanisms or safeguards for the transfer of personal data to third countries that are approved and permitted by the data protection legislation.
4. The Personal Data Controller agrees to further entrust the processing of personal data to such further processors as:
 - a. hosting providers;
 - b. operators responsible for sending email and SMS notifications;
 - c. operators analyzing traffic and user behavior;
 - d. software houses;

- e. lawyers;
 - f. accountants;
 - g. operators responsible for payment processing;
 - h. operators responsible for the issuance and storage of accounting documents, (e.g., Fakturownia);
 - i. internal CRM systems.
5. In a situation in which the Processor intends to further entrust the processing of personal data to a further processor other than the one indicated in paragraph 4, the Processor shall notify the Personal Data Controller of this intention prior to further entrustment. The notification shall be deemed effective if sent to the email address indicated by the Personal Data Controller under the Prime Agreement.
 6. If, upon receipt of the notice referred to in paragraph 5, the Personal Data Controller does not object within 48 (in words: forty-eight) hours after receiving the notice, the Parties shall be deemed to have consented to the intent of the Processor.

§ 11.

Security of personal data processing

1. Throughout the duration of the Entrustment Agreement, the Processor shall be obliged to implement and maintain appropriate technical and organizational measures that ensure the degree of security of personal data processing corresponding to the risk of violation of the rights and freedoms of the persons whose personal data are processed.
2. In a situation in which, for instance, due to the nature of the entrusted personal data or personal data processing processes, it will be necessary to implement additional security measures, due to the individual situation of the Personal Data Controller, the Parties shall agree on the principles of implementing such security measures, provided that the cost of implementing additional security measures in each case shall be borne by the Personal Data Controller.

§ 12.

Notification of suspected data breaches

1. The Processor shall notify the Personal Data Controller of any suspected breach or finding of a personal data protection breach — no later than 48 (in words: forty-eight) hours after becoming aware of the suspected breach or finding of a personal data protection breach. The notice shall be addressed to the email address designated by the Personal Data Controller under the Prime Agreement.
2. In the notification, the Processor shall indicate the circumstances of the incident, the probable causes, and the measures that have been applied or should be applied in connection with the incident in order to minimize the negative effects on data subjects.
3. The Processor is obliged to provide the Data Controller with the opportunity to participate in the clarification of the circumstances of the incident.
4. If a breach or suspected breach of personal data protection has been caused by the Personal Data Controller or other processors, but within the scope of personal data entrusted to the Processor, the Personal Data Controller shall notify the Processor no later than 48 (in words: forty-eight) hours from the moment of acquiring such information.
5. In the event of a breach of personal data protection that:
 - 1) arose due to the sole fault of the Personal Data Controller, within the scope of data entrusted to the Processor — the costs of handling the breach shall be borne by the Personal Data Controller;
 - 2) occurred due to the sole fault of the Processor, in the scope of data entrusted to the Processor — the cost of handling the breach shall be borne by the Processor;
 - 3) arose through the fault of both the Personal Data Controller and the Processor — the cost of handling the breach shall be borne by both Parties, in proportion to the degree of contribution to the breach.

§ 13.

Control of the Processor

1. The Personal Data Controller shall have the right to inspect whether the measures applied by the Processor in processing the entrusted data correspond to the Entrustment Agreement, and to conduct an audit.
2. In order to exercise the right of audit, the Personal Data Controller shall submit a notice of intent to audit well in advance of not less than 14 (in words: fourteen) calendar days before the planned audit. Such notice shall be provided electronically to the email address designated by the Processor.
3. The audit shall be conducted at the expense of the Personal Data Controller, which shall include the remuneration of the appointed auditor, as well as the costs of the Processor related to the time commitment and delegation of the relevant personnel of the Processor — the Personal Data Controller will be charged with the costs of the Processor according to the standard hourly rates used by the Processor.
4. The audit shall be conducted in accordance with the personal data protection regulations, the Processor's internal procedures and policies, and the rules regarding the manner and scope of conducting the audit agreed in advance by the Processor with the Personal Data Controller. In the event that the Personal Data Controller outsources the audit to an auditor, the condition for conducting the audit is that the auditor and the Processor first conclude a confidentiality agreement, with the content specified by the Processor; whereby the conclusion of the agreement may also consist of the acceptance of separate rules and regulations.
5. The Processor shall have the right to refuse, to the reasonable extent, to provide the Personal Data Controller or the auditor with information, access to materials or their facilities for the audit where, in the Processor's opinion, this could pose a threat to the security (confidentiality, availability, or integrity) of the Processor's data or their customers, including, in particular, by revealing organizational or technological solutions used by the Processor to protect personal data, and thus contribute to reducing the level of protection of any personal data processed by the Processor; or where this could result in a threat to the Processor's business secrets.
6. Any persons (other than persons employed by the Processor) conducting an audit at the Processor's premises or systems shall comply with the data security policies in effect at the Processor's organization, which shall be confirmed in writing by the persons conducting the audit prior to the commencement of the audit in question.

§ 14.

Duty to cooperate

1. The Processor shall, to the extent possible, cooperate with the Personal Data Controller in the exercise by data subjects of the rights provided for in Articles 13–22 of Regulation 2016/679. In particular, the Processor shall:
 - a. provide all information and explanations necessary for the exercise of the data subject's rights;
 - b. meet the deadlines related to the exercise of the data subject's rights.
2. The Personal Data Controller shall be the entity solely competent and responsible for responding to inquiries and requests for the exercise of data subjects' rights, including requests for access, rectification, deletion, erasure, transfer, or restriction of personal data processing.
3. If a data subject makes a direct request to the Processor to exercise their rights, the Processor shall forward such request to the Personal Data Controller to deal with the matter.
4. At the request of the Data Controller, notified well in advance, not less than 3 (in words: three) working days, the Processor shall provide assistance to the Data Controller, as far as possible:
 - a. in dealing with requests for the exercise of the rights of data subjects;
 - b. in assisting them in compliance with the obligations set forth in Articles 32–36 of Regulation 2016/679;— with the proviso that in these cases, the Processor may require the Personal Data Controller to pay the reasonable costs of such assistance, at the standard hourly rates applied by the Processor. The assistance shall be provided taking into account the nature of the processing and the information available.

5. The Processor shall cooperate with the Personal Data Controller in all contacts of the Personal Data Controller with the President of the Personal Data Protection Office, as well as participate in all inspection activities conducted by the President of the Personal Data Protection Office, to the extent related to the entrustment of personal data processing to the Processor — with the proviso that the Personal Data Controller shall be obliged to cover the documented costs of the Processor related thereto.

§ 15.

Liability

1. The Personal Data Controller shall be liable for failure to perform or improper performance of their obligations under the Entrustment Agreement, and in particular shall be held liable for:
 - a. processing of personal data in violation of personal data protection regulations or in violation of the Entrustment Agreement;
 - b. entrusting the processing of personal data in violation of personal data protection regulations;
 - c. failure to comply with information obligations to the Processor under the Entrustment Agreement;
 - d. failure to give required advance notice of inspection activities;
 - e. evasion of interaction with the Processor;
 - f. failure to reimburse costs they are obligated to reimburse.
2. The Processor shall be liable for failure to perform or improper performance of their obligations under the Entrustment Agreement, and in particular shall be held liable for:
 - a. processing of personal data in violation of personal data protection regulations or in violation of the Entrustment Agreement;
 - b. failure to ensure an adequate level of security of personal data processing;
 - c. failure to notify the Personal Data Controller of a suspected or confirmed breach of personal data protection;
 - d. evasion of cooperation with the Personal Data Controller.
3. With respect to the performance of the Entrustment Agreement, the Processor shall be held liable to the Personal Data Controller only for events that occur due to the sole fault of the Processor, which in particular means that the Processor shall not be held liable for damages arising due to the act, omission, or contribution of the Personal Data Controller or third parties for which the Processor is not responsible, or the occurrence of force majeure. In the case of using another entity to perform the Prime Agreement (e.g., subcontractors), the Processor shall not be held liable for the acts or omissions of the other entity to the fullest extent permitted by law.
4. The Processor's total liability to the Personal Data Controller for breach of the Entrustment Agreement shall be limited in accordance with the provisions of the Prime Agreement — provided that the limitation of liability shall not apply to damage in respect of which, in accordance with mandatory provisions of law, liability cannot be excluded or limited, in particular damage caused intentionally.
5. In the event that the Processor incurs any costs related to a breach of the Entrustment Agreement by the Personal Data Controller, and in particular the Processor pays compensation to a third party for property damage or non-property damage resulting from a breach of the personal data protection laws, then the Personal Data Controller shall reimburse the Processor, on a recourse basis, the equivalent of all documented costs, in particular the equivalent of the compensation paid — unless the damage suffered by the third party resulted from an event for the occurrence of which the Processor can be held solely responsible.
6. In the event that an administrative fine is imposed for reasons attributable to the Personal Data Controller, the Processor shall be entitled to demand that the Personal Data Controller refund all or part of the fine.

§ 16.

Final provisions

1. The headings of editorial units (paragraphs) used in the Regulations are informative for the convenience of the Parties and do not affect the interpretation of the Regulations, as well as the order in which they are arranged.
2. The law applicable to the Regulations shall be Polish law.

3. Matters not regulated by the provisions of the Regulations shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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) (OJ EU L of May 4, 2016), the Act of May 10, 2018 on the protection of personal data (OJ 2019, item 1781, as amended), the Act of April 23, 1964 of the Civil Code — Civil Code (i.e. Journal of Laws 2022 item 360, as amended), and other applicable laws.
4. In the event of any disputes arising between the Parties regarding the conclusion, interpretation, performance, and legal effect of the Entrustment Agreement, the Parties shall in good faith enter into negotiations to resolve the dispute amicably. If the dispute is not resolved amicably, the Parties shall submit the dispute for settlement to a court of competent jurisdiction over the registered office of the Processor.
5. The Processor reserves the right to amend the Regulations, including during the execution of the Prime Agreement. Each document is marked with the date from which its provisions are effective.
6. The Personal Data Controller shall be notified of the planned change in the content of the Regulations by email sent to the email address indicated by the Personal Data Controller.
7. The Personal Data Controller will be notified of changes to the Regulations at least one week in advance.
8. The Regulations are effective as of August 1, 2022.