The data processing agreement between the Controller and the Processor pursuant to Article 28(3) of the General Data Protection Regulation shall be concluded between

**the Processor** (${cpc\_01\_a})

and

**the Controller** (${cpc\_01\_b})

Introductory provisions

The Controller wishes to contract the performance of the services referred to in Article 3 of this Agreement with the Processor. Contracted services include the processing of personal data. General Data Protection Regulation (GDPR), in particular Article 28 of the GDPR lays down certain requirements regarding the processing of personal data that the Processor is required to comply with on behalf of the Controller. In order to ensure the fulfilment of these requirements, the Parties shall conclude this Agreement.

Art. 1 Definitions of terms

The terms used in this Agreement and defined in the articles of GDPR shall have the meaning as set out in the applicable provisions of the GDPR.

Art. 2 Representatives in the territory of the European Union

According to the provisions of Article 27 (1) in accordance with Article 3 of the GDPR, the Processor has chosen as a representative within the territory of the European Union: ${cpc\_25}

3. Subject matter of the Agreement

3.1. On behalf of the Controller and on the basis of the Main Contract concluded on day/month/year (the “Main Contract”), the Processor will provide services to the Controller in the following areas:

${cpc\_02\_b}

* ${cpc\_02\_b\_item}

${/cpc\_02\_b}

For this purpose, the Controller shall provide the necessary personal data to the Processor who will process the data solely on behalf of the Controller and under instructions given by the Controller, unless otherwise provided by European Union law or by the legal provisions of the Member State law applicable to the Processor. The purpose and scope of the processing of personal data by the Processor are determined by the Main Contract and instructions of the Controller are described in Appendix 1 to this Agreement. The Controller is responsible for the lawfulness of the data processing according to Article 6 (1) of the GDPR.

3.2. The Parties agree to regulate their relationship with regard to the rights and obligations under the applicable regulations in the field of personal data protection by this Agreement. In case of doubt, the provisions of this Agreement shall prevail over the provisions of the Main Contract.

3.3. The provisions of this Agreement are applicable to all activities undertaken in connection with the Main Contract by the Processor, its employees or agents with regard to personal data originating from the Controller, which is collected for, or processed on behalf of the Controller.

3.4. This Agreement shall apply during the period of application of the Main Contract, unless any of the following provisions provide for further obligations or the right to terminate the Agreement.

3.5. Any agreed processing of personal data will take place exclusively on the territory of a Member State of the European Union or on the territory of a Member State of the European Economic Area. The relocation of any part of the service or of the whole service to a third country may only be allowed if the conditions set out in Article 44 of the GDPR are met and, if there is a prior agreement with the Controller, in written or documented electronic form.

Art. 4 Categories of data processed and categories of data subjects

4.1. Acting under the Main Contract, the Processor will be given access to personal data specified in Appendix 1 and belonging to the categories of data subjects also specified in Appendix 1.

${cpc\_03}

Art. 5 Controller’s instructions to the Processor

5.1. The Processor may collect, use or otherwise process personal data within the scope of the Main Contract and in accordance with the instructions of the Controller, in particular as regards the potential transfer of data to a third country or to an international organisation. If the Processor needs to further process the data on the basis of an obligation under European Union or Member State law applicable to the Processor, the Processor shall notify the Controller of those obligations before starting such processing.

5.2. The Controller’s instructions to the Processor shall initially be governed by this Agreement, but these instructions may be amended, supplemented, or replaced by individual instructions in a written or documented electronic format. The Controller has the right to issue such instructions at any time. Amendments may include instructions on rectification, erasure and suspension of data processing. Persons authorised to issue or receive instructions shall be specifically indicated in Appendix 5 to this Agreement. In the event of a change or long-term inability of authorised persons, the Parties shall communicate who their deputies are to the other party without delay.

5.3. The Controller and the Processor shall document all instructions issued to the Processor and shall keep the said documentation for the duration of this Agreement and five years later. Instructions relating to the period after the expiration of the Main Contract will be considered as an amendment to the instructions. The provisions of this Agreement shall not affect the possible reimbursement of additional costs arising from such additional instructions issued by the Controller to the Processor.

5.4. If the Processor suspects that the instructions given to him by the Controller are not in accordance with the regulations in the field of personal data protection, the Processor shall immediately notify the Controller thereof. The Processor shall have the right in such a case to defer the application of such instructions until the Controller has received confirmation or modification of such instructions. The Processor has the right to refuse instructions from manifestly illegal content.

Art. 6 Processor’s protective measures

6.1. The Processor shall act in accordance with legal requirements in the field of personal data protection and shall not transfer or make available to third parties data originating from the Controller. The Processor shall take measures in accordance with industry security and information security standards to adequately protect the data and documents against unauthorised access and other risks to the confidentiality and integrity of the data.

6.2. As regards responsibility for the processing operations in which it participates, the Processor shall organize its internal organization in a manner that complies with the requirements in the field of personal data protection. In particular, the Processor shall ensure adequate implementation of all necessary technical and organisational measures in accordance with Article 32 of the GDPR, and in particular the measures indicated in Appendix 2 to this Agreement. Regarding the processing of special categories of personal data, the Processor shall further implement the technical and organisational measures prescribed by the national regulation on the protection of personal data applicable to the Controller. At the request of the Controller, the Processor shall provide the Controller with detailed information on how the listed technical and organisational measures have been determined and implemented. The Processor shall have the right to modify the implemented security measures provided that this does not jeopardise the agreed level of protection.

${cpc\_24}

6.4. Employees of the Processor performing tasks related to the processing of personal data for the Processor are prohibited from collecting, using or other processing of personal data without authorisation. The Processor shall ensure that all employees involved in the processing of personal data and the fulfilment of this Agreement sign an appropriate confidentiality agreement in accordance with the provisions of Article 28 (3)b of the GDPR. The Processor has the task of adequately educating and instructing employees about the existence of specific obligations in the field of personal data protection arising from this Agreement, as well as the existing limitation of the purpose of personal data processing and the obligation to comply with the instructions. The Processor shall ensure that these obligations continue after the expiry or termination of this Agreement and after the termination of the employment relationship of the employee with the Processor. The Controller may request, and the Processor is obliged to provide evidence that these obligations are fulfilled in an adequate manner.

6.5. The processing of personal data on the basis of this Agreement by employees in their homes or other private premises (remote work/home office of employees of the Processor) is permitted only with the consent of the Controller. If personal data are processed at the employee’s home, the Processor shall contractually ensure access to that area for the purpose of monitoring the security of the processing of personal data, in particular the application of appropriate technical and organisational measures in accordance with the provisions of Articles 6 (1) and 6 (2) of this Agreement and the provisions of Article 32 of the GDPR.

Art.7. Processor’s information obligations to the Controller

7.1. In the event of interference, suspected data breach, breach of contractual obligations by the Processor, suspected security incidents or other irregularities in connection with the processing of personal data by the Processor, by persons in charge of the Agreement or by third parties, the Processor shall without delay inform the Controller in writing or in documented electronic form. This also applies in the case of supervision carried out by the Agency for the Protection of Personal Data or other supervisory authority in the field of personal data protection. To the extent possible, the notification of a possible infringement should contain the following information:

1. Description and nature of the personal data breach, in particular which categories of personal data and data subjects are potentially affected by the breach and the number of personal data concerned
2. A description of the possible consequences of the personal data breach; and
3. Description of the measures taken or proposed by the enforcer to mitigate the consequences of the personal data breach and prevent future breaches

7.2 The Processor shall without delay take all necessary measures to protect the personal data and prevent possible further adverse consequences for the rights and freedoms of the data subject. The Processor will inform the Controller of the measures taken and request further instructions.

7.3. In the event that the data breach referred to in Article 7 (1) of this Agreement also concerned the data of the Controller, the Processor shall provide the Controller with all necessary information without delay.

7.4. If necessary, the Processor will adequately assist the Controller in ensuring compliance with the Controller’s obligations under Articles 33 and 34 of the GDPR. The Processor shall make the notification of the breach on behalf of the Controller upon receipt of instructions in accordance with Article 5 of this Agreement.

7.5. In the event that the data of the Controller are potentially compromised by the seizure or confiscation of objects carried out by the Processor as a result of enforcement, bankruptcy or bankruptcy settlement or other events or measures taken by a third party, the Processor shall notify the Controller of such proceedings without delay, unless it is prevented by a decision in judicial or administrative proceedings. In such a case, the Processor shall immediately inform all relevant authorities and organisations that, under the provisions of the GDPR, the Controller has the exclusive right to take decisions with regard to personal data.

7.6. In the event of significant changes to the security measures set out in Article 6 (2) of this Agreement, the Processor shall inform the Controller without delay.

7.7. In the event of a change of person performing the tasks of a data protection officer or data protection adviser, the Processor shall inform the Controller without delay.

7.8. The Processor, and if applicable its representative, shall keep a record of the processing activities for all processing carried out on behalf of the Controller in accordance with the requirements of Article 30 (2) of the GDPR. The Processor shall provide, upon request, a record of the processing activities to the Controller.

7.9. The Processor shall assist the Controller adequately with the completion of its record of processing activities, as well as assistance in carrying out the data protection impact assessment carried out by the controller pursuant to Article 35 of the GDPR. The Processor will also assist the Controller in the process of prior consultation with the supervisory authority pursuant to Article 36 of the GDPR. In both cases, the processor will adequately provide the controller with the necessary details.

Art.8. Right of the Controller to control the work of the Processor

8.1. Before starting the data processing, and then regularly during the processing period, the Controller is obliged to verify whether the technical and organisational measures taken by the Processor ensure an adequate level of security of the personal data processing operation. To that end, it may request information from the Processor or request that oversight by independent experts be carried out, the relevant industrial certificates or internal audit results be adopted and verified. The Controller may also, after timely coordination and during normal working hours, personally monitor the technical and organisational measures of the Processor or have them verified by independent experts, unless the latter are in competition with the Processor. The Controller shall control the work of the Processor only to the extent necessary so as not to unnecessarily interfere with the business of the Processor.

8.2. On the basis of oral, written or electronic means submitted to the Controller’s request, the Processor shall inform the Controller in due time of all details and information related to the supervision of the Processor’s technical and organisational measures.

8.3. The Controller will document the findings of the inspection and inform the Processor accordingly. In the event that the Controller detects errors or irregularities in the work of the Processor, in particular as regards the application of the Controller’s instructions, the Controller shall inform the Processor without delay. If it is necessary to modify the instructions or the manner in which the Processor carries out the instructions of the Controller, the Controller shall immediately notify the Processor of those changes.

8.4. At the request of the Controller, the Processor shall provide the Controller with an insight into the data protection system and the verification system of employees’ powers to access the data.

8.5. At the request of the Controller, the Processor shall present to the Controller the documentation on the fulfilment of the obligation laid down in Article 6(4) of this Agreement to ensure the confidentiality of information which employees have become aware of or to which they have access in the performance of their duties.

8.6. *(Optional)* The Controller shall reimburse the Processor for the costs incurred as part of the supervision of the Processor’s work.

9. Selection and contracting of sub-processors

${cpc\_04\_abc}

9.2. Where the Processor contracts with a third party the performance of ancillary tasks, this shall not be considered a sub-contractor within the meaning of the provisions of this Agreement. Such ancillary tasks include postal transport, transport and shipping services, cleaning services, physical security services, telecommunications services that are not related to the services provided by the Processor to the Controller under this Agreement. The maintenance and verification services of IT equipment represent the services of sub-processors and require the prior consent of the Controller as they relate to the information systems used in the context of the Processor’s provision of services to the Controller.

10. Requests and rights of data subjects

10.1. The Processor shall assist the Controller by applying appropriate technical and organisational measures to comply with the obligations of the Controller as regulated by Articles 12-22, 32 and 36 of the GDPR.

10.2. If the data subject requests the exercise of his or her rights directly from the Processor, the Processor will not act independently of the Controller, but will refer the data subject without delay to the Controller and await instructions from the Controller on how to proceed.

*(Optional)* 10.3 The Controller shall reimburse the Processor for the costs incurred by supporting the Controller in the fulfilment of the data subject’s request and rights.

11. Responsibility of the Controller and the Processor

11.1. The Controller and the Processor shall be liable towards the data subjects in accordance with the provisions of Article 82 of the GDPR. The Processor will cooperate with the Controller on possible liability cases for damages.

11.2. At the request of the Controller, the Processor shall exempt the Controller from liability for any claims made by the data subject against the Controller arising from a breach of the obligation of the Processor towards the Controller under the GDPR or if the Processor has not acted in accordance with the instructions given to it by the Controller by this Agreement or in particular.

11.3. The parties shall release each other from liability if one of them proves that he or she is not liable for the circumstances that gave rise to the damage to the data subject. In other cases, the provisions of Article 82(5) of the GDPR shall apply.

12. Right to Extraordinary Termination

The Controller may terminate the Main Contract in full or terminate some of its provisions if the Processor fails to fulfil its obligations under the Agreement, if it intentionally or through gross negligence violates the provisions of the GDPR, the national law on the protection of personal data and other laws or regulations relating to the protection of personal data, if it is unable or unwilling to comply with the instructions given to it by the Controller or opposes the exercise of the right of the Controller to supervise the implementation of the processing of personal data in accordance with the terms of this Agreement.

13. Termination of the Contract

13.1. Upon termination of the Main Contract or at any time at the request of the Controller, the Processor shall return to the Controller all documents, data and data media that the Controller has provided to the Processor or delete them at the request of the Controller, unless such erasure is prohibited by the regulations of the European Union or the national regulations of the Republic of Croatia. This obligation also applies to any backup (*backup*) made by the Processor. The Processor should also document and, upon request, provide documentation that it has effectively erased the Controller’s data.

13.2. The Controller shall have the right to verify that the Processor has complied with contractual obligations regarding the return of data or the effective erasure of data. The Controller may entrust such verification to independent experts provided that they are not in competition with the Processor.

13.3. The Processor should ensure the confidentiality of the data which has become known to it in connection with the Main Contract even after the expiry of the main contract. The provisions of this Agreement shall remain in force after the expiry of the Main Contract for as long as the Processor is in possession of the personal data received from the Controller or collected on behalf of the Controller.

14. Closing provisions

14.1. Any amendment to this Agreement shall be in writing or in the form of an electronic document. This Agreement, as well as its Appendices, may be amended or supplemented only by the consent of the contracting Parties.

${cpc\_05}

14.3. Should any provision of this Agreement be either partially or wholly void or unenforceable, this shall not affect the validity and viability of the other contractual terms.

14.4. This Agreement shall enter into force upon signature by the responsible persons of both contracting Parties.

Appendices to this Agreement:

Appendix 1 – Description of categories of data, data enjoying a specific level of protection and data subjects or categories of data subjects

Appendix 2 – Technical and organisational measures applied by the Processor

Appendix 3 – List of persons authorised to issue or receive instructions

Appendix 4 – List of authorised sub-processors

For the Controller:  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
*(Name and surname, function in the organisation)*  
  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(*Place and date, signature)*

For the Processor:  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
*(Name and surname, function in the organisation)*  
  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(*Place and date, signature)*

Appendix 1 – Description of categories of data, data enjoying a specific level of protection and data subjects or categories of data subjects, for example:

Categories of data subjects whose personal data are processed:

${cpc\_06}

* ${cpc\_06\_item}

${/cpc\_06}

Categories of personal data processed

${cpc\_07}

* ${cpc\_07\_item}

${/cpc\_07}

${cpc\_08\_a}

Sensitive data processed (if applicable) and the restrictions or safeguards applied that take full account of the nature of the data and the risks, such as strict purpose limitation, access restrictions (including access only to personnel who have undergone specialized training), records of data access, restrictions on onward transfers or additional security measures

${cpc\_08\_b}

* ${cpc\_08\_b\_item}

${/cpc\_08\_b}

${/cpc\_08\_a}

Nature of personal data processing

* ${cpc\_09}

Purpose for which personal data is processed on behalf of the Controller

* ${cpc\_10}

Processing time

* ${cpc\_11}

If the processing is performed by (sub)processors, state the subject, nature and duration of the processing

* ${cpc\_12}

Appendix 2 – Technical and organisational measures applied by the Processor

1. Pseudonymization and encryption of personal data

${cpc\_13}

* ${cpc\_13\_item}

${/cpc\_13}

2. Physical entry/access control

${cpc\_14}

* ${cpc\_14\_item}

${/cpc\_14}

3. Access control for data processing systems

${cpc\_15}

* ${cpc\_15\_item}

${/cpc\_15}

4. Access control to personal data

${cpc\_16}

* ${cpc\_16\_item}

${/cpc\_16}

5. Controls in the data transfer process

${cpc\_17}

* ${cpc\_17\_item}

${/cpc\_17}

6. Application-level access control

${cpc\_18}

* ${cpc\_18\_item}

${/cpc\_18}

7. Data availability control

${cpc\_19}

* ${cpc\_19\_item}

${/cpc\_19}

Appendix 3 – List of persons authorised to issue or receive instructions

Persons who can issue instructions on behalf of the Controller:

${cpc\_20}

1. ${cpc\_20\_item}

${/cpc\_20}

Persons to receive instructions on behalf of the Processor:

${cpc\_21}

1. ${cpc\_21\_item}

${/cpc\_21}

Communication channels used to send and receive instructions:

${cpc\_23}

${cpc\_22\_a}

Appendix 4 – List of authorised sub-processors

${cpc\_22\_b}

1. ${cpc\_22\_b\_item}

${/cpc\_22\_b}

${/cpc\_22\_a}