Personal Data Processing Agreement

This wording of the Personal Data Processing Agreement (the **Agreement**) has come into effect and applies from 21st of September 2023. This Agreement is concluded between the Service Provider (the **Data Processor**) and the Client (the **Data Controller**) and is an integral part of the Services Agreement.

1. **Terminology:**

   1.1. The terminology used in the Agreement is in line with concepts used in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the **GDPR**).

   1.2. The Parties agree that in cases where the Data Controller resells the Services provided by the Data Processor to the final customers of the Client, the Data Controller may act as a data processor in relation to such customers and the Data Processor may act as an auxiliary data processor (sub-processor) in relation to such customers, but this does not affect the relations between the Parties regulated by this Agreement. In such case, a separate personal data processing agreement will be signed between the Data Controller and such a customer, and the Data Controller has the right to make the Client's customer aware of this Agreement without disclosing confidential information.

2. **The processing of personal data is carried out for the purpose of providing the identification and document signing service.**
3. **In cases where the Client orders the identification and document signing service, the following terms and conditions apply:**

   3.1. The Data Processor undertakes to process personal data only for the purpose of performance of the Services Agreement and in accordance with the instructions of the Data Controller set forth in documents, including this Agreement and its appendices. Detailed information on the processing of personal data is provided in Appendix 1 to this Agreement, which forms an integral part of the Agreement.

   3.2. The Data Controller shall ensure that the processing of personal data, including their transfer to the Data Processor, is and will be carried out in accordance with data protection legislation and the requirements of secure data transfer. The Data Controller is responsible for compliance of the processing of personal data with the applicable data protection legislation with regard to data subjects and the supervisory authority.

   3.3. The Parties undertake:

      3.3.1. to ensure that personal data is processed only for legitimate purposes and under conditions established by the Data Controller, without violating provisions of the GDPR, the Law of the Republic of Lithuania on Legal Protection of Personal Data and other legal acts;

      3.3.2. ensure that personal data are processed accurately, fairly and lawfully;

      3.3.3. to ensure that personal data are protected against accidental or unlawful destruction or against accidental loss, alteration, unauthorised disclosure or unauthorised access to them, in particular where data are transmitted over the network during the processing, as well as against all other unlawful forms of processing, and that these measures provide an adequate level of protection, taking

into account the risks associated with the processing and the nature of the data to be protected, taking into account the state of the art and cost of implementation of those measures;

3.3.4. to ensure the confidentiality of personal data transmitted by the other Party; the data may not be disclosed third parties, and no other opportunity to access the data in any form may be given to third parties, unless otherwise provided for by this Agreement or the legal acts of the Republic of Lithuania; the Parties shall be liable for the confidentiality and security of the obtained personal data from the moment of their receipt.

3.4. The Data Processor undertakes:

3.4.1. to process personal data only on behalf of the Data Controller and in accordance with the instructions of the Data Controller set forth in documents, including this Agreement, and applicable legal acts; if the Data Processor is unable for any reason to ensure compliance with the Agreement or data protection legislation, the Data Processor undertakes to notify the Data Controller thereof as soon as possible, in which case the Data Controller has the right to suspend the transfer of data to the Data Processor, no longer allow the processing of data, and/or to terminate this Agreement;

3.4.2. to ensure that the employees of the Data Processor or other authorised persons who will process personal data have a permanent obligation under confidentiality agreements to ensure confidentiality of personal data received from the Data Controller;

3.4.3. to implement technical and organisational measures to ensure data security prior to the processing of personal data, taking into account the risks associated with the processing, the nature of the data to be protected and taking into account the state of the art and costs of implementation of those measures;

3.4.4. immediately, but no later than within 24 hours from the receipt of the request, to notify the Data Controller of the following (i) any legally binding request by law enforcement authorities to disclose the personal data received, unless this is prohibited; and (ii) any accidental or unauthorised access to the data, the leak of personal data and/or a personal data breach;

3.4.5. to provide the Data Controller with the information and /or documents necessary to ensure that the Data Processor properly complies with the requirements for the protection of personal data set out in the Agreement and legal acts;

3.4.6. to store personal data for no longer than is necessary in accordance with the Agreement and legal acts;

3.4.7. to collect documentation and information on data processing;

3.4.8. to transfer personal data only to the Data Controller or, on behalf of the Data Controller, to a person designated by the Data Controller if such person has the right to receive personal data in accordance with the applicable legal acts of the Republic of Lithuania;

3.4.9. to ensure assistance in exercising the rights of data subjects and in demonstrating compliance with the requirements of the GDPR, carrying out a data protection impact assessment and, if necessary, consulting the supervisory authority;

3.4.10. to refrain from transferring the received personal data to any third parties without the prior written consent of the Data Controller;

3.4.11. to refrain from transferring the received personal data to third countries or international organizations without the prior written consent of the Data Controller;

3.4.12. to respond to all requests of the Data Controller related to processing of personal data in detail no later than within 5 working days and to follow the instructions of the competent supervisory authority regarding the processing of personal data;

3.4.13. to provide the Data Controller with all the information necessary to prove compliance with the obligations set out in this Agreement and the requirements for data processors set out in the GDPR, and to enable and assist the Data Controller or another auditor authorised by the Data Controller in carrying out audits, including inspections. During the audit or inspection, the Data Controller or another auditor authorised by the Data Controller may (among other things) require answers to written or oral questions, submission of documents or other information justifying compliance with the data protection requirements set out in this Agreement or legal acts;

3.4.14. to ensure that auxiliary processors (sub-processors) engaged by the Data Processor assume the same obligations with respect to the Data Processor as applicable to the Data Processor under this Agreement.

3.5. The Data Controller gives general consent to the Data Processor to engage the sub-processors specified in Appendix 1 as well as other sub-processors if this is necessary for performance of the Services Agreement and/or this Agreement. The Data Processor undertakes to inform the Data Controller of any planned changes related to the use or replacement of other data processors, thus giving the Data Controller the opportunity to express its position on such changes.

3.6. The Data Controller undertakes:

3.6.1. to give written instructions to the Data Processor on how and by what means the Data Processor is to process personal data, i.e., specific instructions regarding each processing operation of personal data, if such instructions are not specified in the Appendices to this Agreement;

3.6.2. to lawfully manage and process the personal data provided to the Data Processor, i.e., have a legal basis for the processing of data;

3.6.3. obtaining consents of data subjects (if necessary) before the Data Processor begins processing their data;

3.6.4. provide the Data Processor with the information necessary for the processing of personal data;

3.6.5. having noticed any problems related to the processing of personal data when personal data are processed in accordance with this Agreement, to inform the Data Processor in writing about it without delay;

3.6.6. to inform the Data Processor about the revised, updated or deleted personal data without delay;

3.6.7. to grant the requests of data subjects for exercising of their rights;

3.6.8. to comply with other obligations laid down in the applicable data protection legal acts.

3.7. The parties agree that the competent supervisory authority shall have the right to carry out an audit of the Data Processor in accordance with the applicable data protection legal acts, and such audit would be of the same scale and subject to the same conditions as the audit of the Data Controller.

3.8. The Data Processor reserves the right to make operational and organisational decisions necessary for the provision of the Services to the extent that this does not change the purposes of the processing of personal data.

3.9. To ensure a higher level of data protection, the Parties may take additional measures to protect personal data by agreeing on compensation of the associated additional costs.

3.10. The Parties agree that in the event of termination of provision of personal data processing services, the Data Processor and the sub-processors, if any, will (at the choice of the Data Controller) either return all transferred personal data and their copies to the Data Controller or destroy all personal data and send confirmation to the Data Controller that this has been done, unless the legislation applicable to the Data Processor does not allow for it to return or destroy all transferred personal data or their part. In that case, the Data Processor shall ensure that it will guarantee confidentiality of the personal data transferred and will no longer process the personal data transferred.

4. Liability of the Parties

4.1. Each Party shall be obligated to compensate the other Party for direct losses incurred by it if the first Party has improperly performed its obligations under this Agreement or violated the legal acts governing the processing of personal data. Neither Party shall be liable for indirect losses of the other Party that may relate, among other things, to lost profits or savings, deterioration of business reputation, loss of customers, lost income, loss or decrease in business or production, loss or damage to data or files, unless such limitation of liability is prohibited by law.

4.2. In any case, the Data Processor's liability for damages is limited and may not exceed the remuneration received by the Data Processor during the last 12 (twelve) months for the Services provided to the Data Controller and/or its customers under the Services Agreement, unless such limitation is prohibited by law.

5. Final provisions

5.1. This Agreement and its appendices are an integral part of the Services Agreement. In the event of inconsistencies between the Services Agreement and this Agreement, the provisions of this Agreement shall apply.

5.2. This Agreement and personal data processing shall be governed by the legal acts of the Republic of Lithuania.

5.3. This Agreement shall enter into effect from the moment of ordering the Services and shall remain in effect for as long as the Services Agreement is valid. Termination of the Services Agreement automatically means termination of this Agreement.

5.4. The Data Processor reserves the right to amend terms of this Agreement. Amendments or supplements to the Agreement shall take effect only if the Data Controller was notified 30 (thirty) calendar days in advance and the Data Controller has not expressed an objection. If the Data Controller expresses an objection to the amendment to the Agreement, the version of the Agreement that was in effect at the time of the ordering of the Services shall remain in effect with respect to the Data Controller.

5.5. All disagreements and disputes shall be resolved by negotiation. In case of failure to reach an agreement, disagreements shall be resolved in the procedure established by the laws of the Republic of Lithuania at court of the Republic of Lithuania.

5.6. In case of any questions regarding this Agreement and the processing of personal data under it, you may contact the Data Processor's Data Protection Officer (DPO) by e-mail: info@markid.lt.

Appendix 1 to Personal Data Processing Agreement

1. Information on the processing of personal data

1.1. The purpose of the processing of personal data by the Data Processor is:

1.1.1. provision of document signing service.

1.2. The processing of personal data by the Data Processor is mainly related to (the nature of the processing):

1.2.1. data processing operations: collection, recording, accumulation, storage, classification, structuring, combination, alteration (supplementing or rectification), provision, use, search, erasure or destruction.

1.3. The data processing concerns the following personal data:

1.3.1. a name, surname, personal identification number, telephone number, date and time of the session, other personal data, if their processing is necessary for the provision of the Services. Validation of a qualified certificate.

1.4. The data processing concerns the following categories of data subjects:

1.4.1. customers of the Data Controller, customers of the Client of the Data Controller, employees of the Data Controller, business associates of the Data Controller.

1.5. The Data Processor may process personal data on behalf of the Data Controller when the Agreement come into effect. Duration of data processing:

1.5.1. the data shall be stored during the term of the Agreement.

1.6. After the entry into effect of the Agreement, the Data Controller allows the use of these sub-processors:

Name, first name, surname	Entity number	Registered office address	Description of the processing of personal data
SK ID Solutions, AS	10747013	Pärnu mnt 141 11314 Tallinn Estonia	When the Data Processor provides services under Agreement No. 1910/269138, the data sub-processor provides identity authentication services SmartID, Mobile-ID, and manages personal data of the persons authenticated via SmartID, Mobile-ID. It also provides document authentication services.
Identitrade, UAB	304478730	Saltoniškių g. 2-1, LT-08126 Vilnius	When the Data Processor provides services under Agreement No. 20220202-091516721, the data sub-processor provides identity authentication services ZealiD, and

			manages personal data of the persons authenticated via ZealiD.
Amazon Web Services EMEA SARL, (“AWS Europe”)	-	38 avenue JohnF. Kennedy, L-1855, Luxembourg	Backup copies are stored when the Data Processor provides a service.
Rakrėjus, UAB	303126701	J. Kubiliaus st. 6, LT-08234 Vilnius	When the Data Processor provides services under Agreement No. 2021/09/09, the database and documents are stored in the infrastructure provided by the data sub-processor.

2. Personal data security

2.1. The data processor applies the following technical and organisational security measures:

2.1.1. Software and system security:

2.1.1.1. regular software updates;

2.1.1.2. ongoing vulnerability monitoring.

2.1.2. Infrastructure and server security:

2.1.2.1. servers are stored in a Tier III data centre.

2.1.3. Data protection:

2.1.3.1. ongoing data encryption;

2.1.3.2. secure SSL data transfers;

2.1.3.3. encrypted external access via VPN.

2.1.4. Data integrity and recovery:

2.1.4.1. regular data backups.

2.1.5. Access control:

2.1.5.1. Segregated access rights by role;

2.1.5.2. data-level classifications with described usage procedures;

2.1.5.3. resource and asset management procedures.

2.1.6. Access control:

2.1.6.1. documented access rights processes;

2.1.6.2. use of data processors which ensure protection of personal data.

2.1.7. Audit and compliance:

2.1.7.1. compliance with ISO/IEC 27001 standard;

2.1.7.2. Annual security audit by the Security Committee in accordance with the requirements of the ISO / IEC 27001:2013 standard.

2.2. The Data Processor hereby undertakes to comply with iso/IEC 27001 standard for information security management, among other technical and organizational measures specified in the Agreement.