aIDentix Privacy Policy

By clicking "Agreed," "Begin Verifying", "Start Verifying" or similar actions, or by using the aIDentix Services, you agree to enter a legally binding contract with aIDentix (the "Service Provider") for the purpose of using the aIDentix identity verification and KYC service (the "Service") and declare that you are at least 18 years old or have the consent of a parent/guardian to use the Service. If you do not agree to these Terms, do not click "Agreed" (or similar), and do not access or otherwise use any of our Services.

I. General Terms

This Privacy Policy applies to **"aIDentix" Ltd.,** a Bulgarian company registered in the Commercial Register at the Registry Agency under **UIC 204788710**, with mailing address: **5A Baku str, floor 6, 1700 Sofia, Bulgaria, email: office@aidentix.com** ("aIDentix", "Service Provider", "we," "us," or "our") and describes how we collect, use and disclose personal data when providing our identity verification and digital KYC services ("Services"). We verify the identity of individuals ("End Users") as defined in the General Terms and Conditions for Corporate Clients as contractors under contract with our Corporate Clients.

All data processed by aIDentix is stored within the European Union (EU) in compliance with the General Data Protection Regulation (GDPR) and other applicable EU privacy regulations.

II. Service Provided on Behalf of Corporate Clients

- aIDentix provides digital identity verification and KYC services as a contractor under a contract with Corporate Clients. This means that your use of the Services as an End User is in connection with a request for verification of your identity by a Corporate Client of aIDentix.
- Once the identity verification process is completed - whether approved, rejected, or cancelled - **aIDentix retains and processes this information as a Controller**. The relevant information may also be shared with the requesting Corporate Client, who will process it in accordance with their own privacy policies.

III. Personal Data We Collect and Process

- The types of personal data we collect depend on the information required for the identity verification process. We may collect and process the following categories of personal data:
- **Name and Personal No**

- **Contact Information** (such as email address and phone number)
- **Demographic Data** (such as date of birth, nationality, etc.)
- **Government Identification Documents** (such as your ID card or passport, including any personal data contained in the NFC chip pursuant to Article 5 of the Terms of Use of the aIDentix Service for End Users, if applicable)
- **Biometric Information** During the digital identification process, we collect and process the following types of biometric data:

  (i) Scanning your face from the selfie or video you provided;

  (ii) Image of the face from an identity document provided by you (passport or identity card);

  (iii) Data related to the biometric characteristics of your face, which will be compared between the selfie/video and your identity document to confirm your identity.

- **Identifiers and Device Information** (such as your IP address, device type, and operating system)
- **Geolocation Data** (inferred from your IP address, but we do not collect precise location data)

This data is necessary to ensure the accuracy and security of the identity verification process.

IV. How We Use Your Personal Data

Types of Data Collected

- **Identification Document Information:** We collect data from your identification document (such as ID card or passport), which may include:

i. Document type

ii. Document number

iii. Place of issue of the document and date of expiry

iv. Full name

v. Personal identification number (such as PIN, Personal No/EGN, SSN, or other, as applicable)

vi. Date of birth

vii. Nationality

viii. Other identifying information from the document or NFC chip (if applicable)

- **Selfie or Video Data:** We collect a selfie or video solely for the purpose of verifying that you are the individual depicted in your identity document and to perform biometric checks for facial recognition and liveness verification. This information includes:

  (i) A selfie or video submitted by you and/or

  (ii) The photo from the identity document

- **Questionnaire Responses:** We collect responses from additional questionnaires provided during the know your customer "KYC" process, which may require: additional personal data to confirm your identity, necessary to comply with legal or regulatory obligations.

- **IP Address and Browser Data:** We automatically collect and process technical data arising in connection with your use of the Service, including:

  (i) IP address

  (ii) Device type and model

  (iii) Browser type and version

  (iv) Operating system

  (v) Other technical information related to your access and use of the Service

- **Other data related to the use of the Service:** We also collect data about how you interact with our services, including:

  (i) Time taken to complete the identity verification process

  (ii) Access times and interaction data (e.g., customer behaviour, button clicks, mouse hovering, etc.)

For what purpose do we use your data

- **Identity Verification:** To verify the authenticity of your identification document and confirm that you are the individual represented in it. We use biometric information to verify your identity by:

- Comparing the biometric characteristics of the face in your identity document with the biometric characteristics of the face extracted from the selfie or video you provided.

- Establishing a match between the two images as belonging to the same individual.

- Liveness **Detection**: We process your biometric data to perform **liveness detection**, ensuring that the person providing the selfie or video is physically present and not

attempting to deceive the verification process through the use of photos or other fraudulent means.

- **Fraud Detection and Prevention**: Biometric information is used to detect and prevent fraudulent activity. By comparing the facial data extracted from the identity document with a selfie or video recording taken by the End User, it is confirmed that only real individuals can complete the identity verification process. We aim to detect and prevent fraudulent activities, including the use of fake or stolen identity documents, as well as attempts to impersonate someone else. We use technical data, such as IP addresses, browser information, and service usage patterns, to identify suspicious behaviour.
- **Compliance with Legal Obligations**: We process data for the purpose of complying with applicable laws and regulatory requirements, such as applicable anti-money laundering (AML) laws and know your customer (KYC) laws. This may include collecting personal data through questionnaires as required by our Corporate Clients.
- **Service Improvement**: We process data in order to improve and refine the services we provide by analysing how they are used, identifying difficulties or inefficiencies in the verification process, and performing optimizations based on feedback and performance indicators.
- **Protection of rights and security:** We process data when necessary to establish, exercise, or defend legal claims, as well as to investigate, prevent, or take action regarding illegal activities, suspected fraud, violations of our terms and conditions, or other situations that could pose a risk to the rights, property, or safety of any party.

Legal Basis for Processing

- Consent: We rely on your explicit consent to process your biometric data (selfie or video) for facial recognition and identity verification purposes.
- Legitimate Interest: We process other personal data, such as your identification document details, IP address, and browser data, based on our legitimate interest in:

  (i) Providing secure and reliable identity verification services

  (ii) Prevention, detection and investigation of fraud

  (iii) Ensuring the integrity, security and continuity of our services

Compliance with Legal Obligations: We may also process your personal data to comply with our legal and regulatory obligations, particularly those related to anti-money laundering (AML) and know-your-customer (KYC) laws.

V. Data Sharing

- We share your personal data under the following circumstances:
  - **With the Corporate Client**: After the identity verification process is finished, we share the verification results, including any personal data, with the Corporate Client that requested the verification.
  - **With Service Providers**: We may provide personal data to trusted third-party service providers who assist in the performance of activities related to identity verification or secure data storage. These providers act as processors of personal data on our behalf and on our instructions, in accordance with personal data processing agreements that include obligations to comply with high standards of security and confidentiality, in accordance with applicable personal data protection legislation.
  - **Legal Obligations**: We may disclose personal data when necessary to comply with a legal obligation, including in response to valid requests from competent authorities, court orders, or other applicable legal processes.

VI. Data Retention

We retain personal data for as long as necessary to provide the Services and comply with legal obligations. This includes retaining data:

- **For Identity Verification**: We retain your data necessary for identity verification, including biometric data, for the duration of the identity verification process and up to 60 days after the process is completed.
- **For Legal Compliance**: We may retain certain data for a longer period, but no longer than 5 (five) years, in accordance with our obligations under applicable anti-money laundering (AML) and financial regulations This retention period allows us to comply with legal obligations for record keeping and assist in the detection of fraud, audits, or investigations by competent authorities.

Throughout the entire retention period, we apply strict access control, encryption, and data minimization principles to ensure the security and confidentiality of your biometric data.

Once we no longer need your personal data for these purposes after the retention period has expired the biometric data is erased in a secure and irreversible manner, and other personal data is erased or anonymized unless otherwise required by law or regulatory inquiry.

VII. Your Rights

Under the GDPR and other applicable EU laws, you have the following rights regarding your personal data:

- **Access**: You have the right to request access to the personal data we hold about you.
- **Correction**: You may request corrections to any inaccuracies in your personal data.
- **Deletion**: You may request the deletion of your personal data, subject to certain legal obligations.
- **Objection and Restriction**: You have the right to object at any time to the processing of your personal data on the basis of legitimate interest, under the conditions of Article 21 of the GDPR, as well as to request the restriction of their processing or to withdraw your consent. In the event of such an objection, we will cease processing unless we can demonstrate that there are legal grounds that take precedence over your interests and rights, or if the processing is necessary for the establishment, exercise, or defence of legal claims.
- **Portability**: You may request that your personal data be transferred to another service provider in a standardized format.

To exercise any of these rights, please contact us at privacy@aidentix.com.

VIII. Data Security

- We implement the necessary technical and organizational measures to protect personal data from unauthorized access, disclosure, alteration, or destruction. All personal data processed by aIDentix is stored securely within the EU.
- All personal data processed by aIDentix, including identification document information, biometric data (such as facial scans), and usage data (such as behaviour), is encrypted both **in transit** and **at rest** using industry-standard encryption protocols. This ensures that your data remains secure at all times during its transmission and storage.
- We use advanced encryption standards, such as **AES-256**, to protect your data, ensuring that only authorized individuals can access the data while it is stored or being transmitted.
- Access to your personal data is restricted to authorized personnel only. These individuals are bound by strict confidentiality obligations and can only access data as necessary to perform the identity verification process or comply with legal obligations.
- We implement multi-factor authentication (MFA) for access to our systems, ensuring that only verified and authorized personnel have access to sensitive data.
- We continuously monitor our systems for potential security threats and vulnerabilities. Any suspicious activity is investigated and addressed immediately to ensure the safety of your personal data.

- In cases where we are legally obligated to disclose personal data (e.g., in response to a court order), we ensure that such disclosure is performed in a secure and lawful manner, in compliance with data protection regulations.

IX. Data Transfers

All data is processed and stored within the European Union. We do not transfer personal data outside of the EU unless legally required to do so. In such cases, we will ensure that appropriate safeguards are in place to protect your data in accordance with applicable law.

X. Changes to this Privacy Policy

We reserve the right to update this Privacy Policy from time to time as changes occur in applicable law or in the scope of services we offer. In the event of significant changes to this Policy, we will update the date at the footer of this document.

XI. Contact Us

- If you have any questions about this Privacy Policy or your personal data, please contact us at the following email address: privacy@aidentix.com or at the following address: 5A Baku Str., Floor 6, 1700 Sofia, Bulgaria
- To contact our data protection office (DPO) – dpo@aidentix.com