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 digital identity verification and KYC service (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 act on behalf of our Corporate Clients to verify the identities of individuals ("End Users").

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

1. aIDentix provides digital identity verification and KYC services on behalf of our **Corporate Clients**. This means that when you, as an End User, engage with our Services, you are doing so because a Corporate Client has requested that aIDentix verify your identity.
2. 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

3. 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**
    - **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 if applicable)
- **Biometric Information** (such as a selfie or video used for facial recognition and liveness verification)
- **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

4. **Identification Document Information:** We collect data from your government-issued identification document (such as ID card or passport), which may include:
   - Document type
   - Document number
   - Document issues and expiry date
   - Full name
   - Personal identifiable number (such as PIN, EGN, SSN or other)
   - Date of birth
   - Nationality
   - Other identifying information from the document or NFC chip (if applicable)
5. **Selfie or Video Data:** We collect a selfie photo or video for the purpose of verifying that you are the individual represented in the identification document and to perform biometric checks for facial recognition and liveness verification. This information may include:
   - A selfie photo or video that you submit
   - The photograph on your government-issued identification document
6. **Questionnaire Responses:** We collect responses to additional questionnaires provided during the KYC process, which may ask for:
   - Additional personal details to verify your identity

- Information required for compliance with legal or regulatory obligations

7. **IP Address and Browser Data:** We automatically collect technical data from your interaction with our service, including:
   - IP address
   - Device type and model
   - Browser type and version
   - Operating system
   - Other technical information related to your access and use of the service
8. **Service Usage Data:** We collect data about how you interact with our services, including:
   - Time taken to complete the identity verification process
   - Access times and interaction data (e.g., button clicks, hesitations, etc.)
   - Usage patterns to detect and prevent fraudulent behavior

Why We Use Your Data

9. **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 facial geometry of the image in your identification document to the facial geometry extracted from the selfie or video you provide
   - Confirming that both images correspond to the same person
10. **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.
11. **Fraud Detection and Prevention**: Biometric information is used to detect and prevent fraudulent activity. By comparing facial data between the identification document and the selfie or video, we ensure that only genuine individuals can complete the verification process. To detect and prevent fraudulent activities, including the use of forged or stolen identity documents or impersonation. We use technical data, such as IP addresses, browser information, and service usage patterns, to identify and mitigate suspicious behavior.
12. **Compliance with Legal Obligations**: To comply with applicable laws and regulatory requirements, such as anti-money laundering (AML) and know-your-customer (KYC) laws. This

may involve collecting additional personal data via questionnaires as required by our Corporate Clients.

13. **Service Improvement**: To enhance and improve our services by analyzing usage data, identifying bottlenecks or issues in the verification process, and making improvements based on feedback and performance metrics.

Legal Basis for Processing

14. **Consent:** We rely on your explicit consent to process your biometric data (selfie or video) for facial recognition and identity verification purposes.
15. **Legitimate Interest**: We process other personal data, such as your identification document details, IP address, and browser data, based on our legitimate interest in:
    - Providing secure and reliable identity verification services
    - Preventing fraud
    - Ensuring the integrity of our services
16. **Compliance with Legal Obligations:** We may also process your personal data to meet our legal and regulatory obligations, particularly those related to AML and KYC compliance.

V. Data Sharing

17. 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 share personal data with trusted third-party service providers who assist us in performing identity checks or storing data securely. These service providers process data on our behalf under strict confidentiality agreements.
    - **Legal Obligations**: We may disclose personal data where required by law, such as in response to valid legal processes or to comply with legal obligations.

VI. Data Retention

18. 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 for the duration of the identity verification process.

- **For Legal Compliance**: We may retain certain data for a longer period to comply with legal obligations, resolve disputes, and enforce our agreements.

Once we no longer need your personal data for these purposes, we will either delete it or anonymize it.

VII. Your Rights

19. 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 may object to the processing of your personal data or request that its processing be restricted.
    - **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

20. We implement appropriate 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.

21. All personal data processed by aIDentix, including identification document information, biometric data (such as facial scans), and usage data, 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.

22. 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 across networks.

23. 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.

24. We implement multi-factor authentication (MFA) for access to our systems, ensuring that only verified and authorized personnel have access to sensitive data.

25. 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.

26. 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

27. 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, and in such cases, we will ensure that appropriate safeguards are in place to protect your data.

X. Changes to this Privacy Policy

28. We may update this Privacy Policy from time to time to reflect changes in our services or legal obligations. When we make material changes to this policy, we will notify you and update the "Last Updated" date at the top of this document.

XI. Contact Us

29. If you have any questions or concerns about this Privacy Policy or your personal data, please contact us at:

    - For Privacy concerns and this Privacy Policy – privacy@aidentix.com
    - To contact our data protection office (DPO) – dpo@aidentix.com