PXL Vision Privacy Policy PXL Ident

1. The product

PXL Vision provides you with a way to verify your identity for a service that requires ID verification. PXL Vision verifies your identity using the identity document and the data it contains, which is captured by a camera and/or, where applicable, collected via the NFC chip on the identity document, as well as by comparing the photograph on the identity document with a selfie video you have recorded. Once verified, the result can be transmitted by PXL Vision to the service provider for further use of their service. Identification may be required for a legally regulated (e.g. a bank or telecommunications company) or non-regulated use case by the provider (transaction partner) requesting the identification. Identification may also be carried out for a Qualified Trust Service Provider (QTSP) if, for example, you wish to commission the issuance of a qualified electronic signature via their certified infrastructure. Furthermore, depending on the customer's requirements, PXL also provides services for signing digital documents with electronic signatures.

2. General information on data protection

We would like to take this opportunity to inform you about the processing of personal data in connection with the identification procedure and, where applicable, the signature process. In this context, personal data refers to any information relating to an identified or identifiable natural person (hereinafter referred to as the "data subject").
The data controller and the contact for exercising data subject rights is

PXL Vision AG
Rautistrasse 33
8047 Zurich, Switzerland

privacy@pxl-vision.com

3. Applicable law

This privacy policy covers the collection and processing of data in accordance with the provisions of the currently applicable version of the EU General Data Protection Regulation (GDPR) and the currently applicable Swiss Data Protection Act (DSG). The DSG always applies; the GDPR applies in the cases defined by law.

4. Data and categories of data as well as processing purposes

a. Data and categories of data

(1) Personal data / master data (identification data)

The verification of identity documents requires the collection and further processing of the following personal data contained in the identity document being checked. This usually includes:

- Surname, first name, address, date of birth, place of birth, maiden name, and, where applicable, any other personal details contained in the document
- Identity document number, issuing authority, date of issue, expiry date
- Biometric photograph

Furthermore, a selfie video is recorded to verify that the person using the service matches the photograph on the ID document.
Carrying out an optional signature process requires the additional processing of data contained in a document to be signed. This data depends on the content of the specific document to be signed, which is processed by PXL for forwarding to a signature service provider.

(2) Technically generated data (usage data)

As part of our solution, we collect technical device data to ensure the security and integrity of the identification process. This involves recording details of the end device being used, such as browser type, operating system, screen resolution, time zone and other device-specific characteristics.

b. Purposes and their legal basis for which the personal data is processed

(1) Provision of the contractually agreed service

In the following cases, data processing serves to fulfil the contractual obligations towards transaction partners and users, who in turn generally enter into or execute a contract with or on behalf of the data subject. Article 31(2)(a) of the Data Protection Act (DSG) and Article 6(1)(b) of the General Data Protection Regulation (GDPR) apply.

i. Identity verification (master data)

Collection and processing of identification data for the purpose of verifying the authenticity of the identity document and confirming that it belongs to the user. The requirements for identification and the associated data processing and transmission are derived from the relevant legal provisions for the respective use case; in the context of the provision of trust services, for example, these include the Swiss Federal Act and Ordinance on Electronic Signatures (ZertES, VZertES) and, when using trust services in and for the EU, from the eIDAS Regulation and the corresponding technical guidelines.

ii. Provision of services downstream of identification

The collection, processing and transmission of identification data, photographs and the selfie video are carried out for the purpose of providing this data to the transaction partner and, subsequently, where applicable, for the provision of the services separately communicated by the transaction partner. In the event that a trust service is requested, the data is transmitted to the QTSP as the transaction partner for the provision of the trust services.

iii. Provision of signature services

Where users have opted for the provision of signature services, the data and information contained in the electronic document to be signed are collected and transmitted for the purpose of carrying out the electronic signature process by the signature service provider and the issuance of the necessary certificate by a trust service provider.

(2) Legitimate interest

In the following cases, we collect and process data on the basis of a legitimate interest in accordance with Section 31 of the Data Protection Act (DSG) or Article 6(1)(f) of the General Data Protection Regulation (GDPR):

i. Improving the user experience of the WebApp

Use of usage data to improve the user experience of the web application and to prevent and detect misuse and fraud.

ii. Troubleshooting

Usage data for resolving software or process errors. Identification data, including photo files, for error checking following the completion of a verification and transaction. Data is also stored in the event of an unsuccessful verification, so that any subsequent errors or complaints can be dealt with if necessary.

iii. Anonymization

Done for statistical purposes

iv. Processing for quality assurance and development purposes

The data collected as part of the identification and verification process is processed by PXL Vision, as the data controller, for its own quality assurance and improvement purposes, including the further development of recognition algorithms, provided that you were informed of this and of your right to object, as described below, at the start of the identification process. The verification process is based on various complex analysis algorithms involving artificial intelligence (AI) and machine learning. In order to ensure consistently reliable, non-discriminatory and secure analysis results, and in particular to effectively counter new and constantly evolving forms of identity fraud, these systems require constant review and further development using real transaction data. This requires a great deal of illustrative material; the specific individuals are not the focus here. The further processing of the data for these purposes of quality assurance and improvement, including for further development, is carried out on the basis of our overriding legitimate interest (in particular Art. 31(2)(e) DSG) or our legitimate interest (Art. 6(1)(f) GDPR) in maintaining system security and quality, preventing algorithmic discrimination (bias prevention) and continuously combating fraud. For this purpose, the data is stored on separate servers located exclusively in Switzerland, subject to strict technical measures. The data is not traded; it is used solely by PXL Vision and access is strictly limited internally. Neither the data nor the models are published. **Your right to object (opt-out)**: You have the right to object at any time, with effect for the future, to the processing of your data for these purposes of quality assurance and improvement, including for further development. You may submit your objection – even before the identification process begins – by email to privacy@pxl-vision.com or by post. Such an objection expressly does not lead to the termination of the identification process and has no adverse effects on the performance of the identification service you have commissioned.

(3) Consent

In the following cases, we collect and process data on the basis of additional consent in accordance with Section 31(1) of the Data Protection Act (DSG) or Article 6(1)(a) or Article 9(2)(a) of the General Data Protection Regulation (GDPR).

i. Implementation of the identification and verification process as well as quality assurance and improvement (biometrics)

In order to verify your identity securely and for the purposes of quality assurance and improvement, including the further development of our recognition algorithms, we process biometric data (from your ID photo and the selfie video). As this involves particularly sensitive or special categories of personal data, we ask you for your explicit consent to this processing during the process for legal reasons. This consent is voluntary; however, without it, it is not possible to carry out the online identification and verification process (for alternative methods, please contact the company for which we are carrying out this process). However, you may withdraw your consent to the processing of your data for quality assurance and improvement, including the further development of our recognition algorithms for the future, or object to such processing, as set out above in 4.b.(2)(iv). The processes used by PXL to process this data are subject to strict data protection requirements and are secured by appropriate technical and organisational security measures.

ii. Processing for the purpose of signing documents

If the document to be digitally signed by users as part of a selected signature process contains special categories of personal data, by authorising the signature process, users consent to the processing of this data for the purpose of signing the document.

5. Recipients or categories of recipients of personal data

a. Transaction partners

Either prior to or following the successful completion of the verification process, the web app will inform you or ask for your consent as to whether the verification result and the data collected may be transmitted to the transaction partner for the purpose of further processing. These are the entities that have commissioned us to carry out the verification and with whom you are conducting a transaction. The transaction partner is solely responsible for processing the data transmitted to them. Please familiarise yourself in advance with their terms and conditions and privacy policy, which will also be displayed to you as part of the overall process.

b. Processor

With the exception of the transaction partner specified during the identification process, PXL will not disclose the data to third parties or make it available to them. However, PXL Vision may engage IT service providers and other data processors. These parties are contractually bound by us to comply with the legal provisions governing data processing and must adhere to the relevant security requirements.

c. Signature Service Providers and Trust Service Providers

Where PXL's services involve carrying out a signature process or creating a qualified electronic signature, the data required for this purpose will be forwarded to a signature service provider and a trust service provider.

d. Authorities

In exceptional cases, it may be necessary to disclose the data we have collected to public authorities, for example in the context of legal proceedings.

6. Storage Duration and Storage Criteria

a. Storage as part of the identification process

Once a transaction has been completed via the web app, the data may be stored in PXL Vision's operational system for a period of up to 12 months, as agreed with the transaction partner, for support and troubleshooting purposes.

b. Storage for Quality Assurance and Improvement

Subject to any objection, as set out above, the data processing involves not only the immediate verification of identity but also the processing of data for the purpose of training our AI algorithmic analysis models within the scope of our legitimate interest. As extensive data sets are required for this purpose, data may be retained for up to seven years. However, in the event of an objection, the relevant data set will be deleted from the database for such uses.

c. Storage for signature processes

If the relevant service is selected, the signature service provider or trust service provider will store the data in accordance with the statutory retention periods applicable in such cases. Further details will be provided separately as part of the signature process.

7. Places of data processing

We generally process your personal data only in Switzerland, Germany and the European Union; however, in exceptional cases, processing may take place in any country worldwide. If a recipient is located in a country without adequate data protection, we contractually oblige the recipient to maintain an adequate level

of data protection (for this purpose, we use the European Commission's revised Standard Contractual Clauses, which are available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?; including the additions required for Switzerland), unless they are already subject to a legally recognised framework for ensuring data protection. We may also disclose personal data to a country without adequate data protection without concluding a separate contract for this purpose, provided we can rely on an exemption provision. An exception may apply, in particular, in the case of legal proceedings abroad, but also in cases of overriding public interest or where the performance of a contract that is in your interest requires such disclosure, where you have given your consent, where it is not possible to obtain your consent within a reasonable period and the disclosure is necessary to protect your life or physical integrity or that of a third party, or where the data in question has been made publicly available by you and you have not objected to its processing. We may also, in certain circumstances, rely on the exception for data from a register provided for by law (e.g. the commercial register) to which we have lawfully gained access.

8. Automated decision-making

As part of the identity verification process, automated procedures are used to verify your identity. The outcome of the identification may lead to automated decision-making by PXL Vision or the transaction partner. Once identity verification is complete, the transaction partner is informed of the result so that they can make a decision based on this information. In some cases, particularly when a QTSP provides identification for a trust service, human intervention by a data processor appointed by PXL Vision or the customer may be required for further verification within the verification process. In the case of automated decisions, you have the right, in accordance with Article 22(3) of the GDPR or Article 22 of the DSG, to a hearing by the data controller to present your point of view and challenge the decision. No profiling takes place.

9. Secure communication

For the transmission of confidential information outside our verification process, we recommend contacting us by telephone, post or via an encrypted contact form. If you contact us via email, social media, messaging services (such as WhatsApp) or by other means, we cannot guarantee complete data security. As part of our data processing, we use specialist providers with highly secure IT infrastructure. These providers are contractually obliged to implement comprehensive technical and organisational measures, such as data encryption (during transmission and storage), strict access controls, adherence to principles such as 'least privilege', and regular security audits in accordance with international standards.

10. Your rights

Under the DSG and the GDPR, data subjects are generally entitled to the following rights, subject to the restrictions provided for by law:

a. Right to withdraw consent and delete personal data concerning you

With regard to the collection of your biometric data, which is based on your explicit consent, you generally have the right to withdraw your consent at any time with effect for the future. You may also generally request the erasure of your data. Withdrawal of consent (or a request for erasure) during the ongoing identification process will result in its immediate termination. Once identification has been successfully completed, a withdrawal will result in the deletion of the data held by PXL Vision, provided there are no mandatory legal retention obligations to the contrary. (Note: If you wish to object solely to the use of your data for quality assurance and improvement purposes, please refer to your right to object under 10.d.).

b. Right of access by the data subject to the personal data concerned

You may at any time request information regarding the processing of your personal data in accordance with Article 15 of the GDPR / Article 25 of the DSG from PXL using the contact details provided above. Please note that in such cases we will take appropriate measures to ensure that you are the person entitled to receive this information.

c. Other rights

You have the right to have inaccurate personal data rectified or incomplete data completed (Art. 32 of the Data Protection Act and Art. 16 of the GDPR). If, during the verification process via the WebApp, you notice an error in the data collected, you should cancel the verification process and inform us via the email address support@pxl-vision.com. Once the data has been transmitted to the transaction partner, please contact them directly as the data controller to have the data corrected.

Under certain legal conditions, you have the right to restrict processing (Art. 30(2)(b) FADP, Art. 18 GDPR; see also the right to object below).

Under certain legal conditions, you have the right to receive or have transferred the personal data concerning you (Art. 28 FADP, Art. 20 GDPR).

d. Your Right to Object

You have the right at any time to object to our processing of your personal data; this applies in particular to any processing of your data for the purposes of quality assurance and improvement, as outlined above. We will then delete your personal data from the database maintained for this purpose and will no longer use it for any further purposes. You can submit such an objection by emailing privacy@pxl-vision.com.

e. Right to lodge a complaint with a supervisory authority

You have the right to lodge a complaint regarding the processing of your data with a supervisory authority; in Switzerland, this is the Federal Data Protection and Information Commissioner (FDPIC), https://www.edoeb.admin.ch. A list of supervisory authorities in the EEA can be found here: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en.

11. Changes to the Privacy Policy

As changes to the law or to our internal processes may require us to amend this privacy policy, we reserve the right to make changes.

PXL Vision AG, June 2026