

Data privacy policy of ti&m AG for online identification and video identification

Version dated 11.10.2022, based on the general privacy policy of ti&m AG.

ti&m AG offers the service to verify official identification documents (especially passports, identity cards and resident permit cards) and to match them with this person ("end customer"). This service is offered by ti&m to clients such as financial institutions and insurance companies in order to comply with legal requirements (e.g., Money Laundering Act, Banking Act) and to increase the security regarding the identity of the end customer. In doing so, ti&m AG acts according to the instructions of its clients as well as the applicable regulatory and legal requirements.

In this privacy statement, we, the companies of the ti&m group (hereinafter collectively ti&m, we or us), explain how we collect and process personal data for online identification and video identification. Personal data means any information relating to an identified or identifiable individual.

In the context of this identification, please provide us only with your own personal data and never with the data of other persons (e.g., family members, data of work colleagues). The identification process can only be carried out on the person in question.

This privacy policy takes into account the EU General Data Protection Regulation (GDPR).

1. Involved companies

The company that uses ti&m's online identification or video identification service to identify its future end customers is the client for the respective identification and is therefore the "data controller" for the entire process under data protection law. In the following, the term controller is used. The controller is the company on whose website or in whose app the identification process is started. The controller's data privacy policy as well as the name of their data protection officer can be found on their website or in their app. In case of ambiguity or to assert your rights, this officer is your primary contact.

In the case of video identification, the Callpoint AG company, Hochbergerstrasse 15, 4057 Basel, carries out the video chat. Under the Data Protection Act, this is the data processor commissioned by the controller. The privacy policy of the Callpoint company can be found here: <https://www.callpoint.ch/en/terms-of-use-and-privacy-policy>.

In turn, ti&m is a data processor of Callpoint or the controller, depending on whether it is a video or an online identification. ti&m keeps the collected data only for a very short time (see Section 7. Duration of retention of personal data) and hands it over to the controller at the end of the process.

Towards the end of the process, a qualified electronic signature is created for the new end customer by Swisscom Trust Services AG, Hardturmstrasse 3, 8005 Zurich, Switzerland, a recognized signature provider. For this purpose ti&m forwards all collected data to Swisscom. The corresponding privacy policy can be found here: <https://trustservices.swisscom.com/en/swisscom-privacy-policy/>.

For the verification of addresses, data is retrieved from the systems of the Swiss or German Post. No personal data is transferred in this case, only the address information. The respective data privacy policies can be found here: <https://www.post.ch/en/pages/footer/data-protection-and-disclaimer>, <https://www.deutschepost.de/en/f/footer/data-protection-and-cookies.html>.

The servers of ti&m AG are located in the data centers of Green Datacenter AG, Industriestrasse 33, 5342 Lupfig, on the one hand and SIX Management AG, Hardturmstrasse 201, 8005 Zurich, on the other. However, these data center operators are not involved in the data processing and have no access to the data.

2. Data protection officer

If you have any data protection concerns, you can always contact the controller's data protection officer, see Section 1. This is your main contact.

If you have concerns about video identification, your contact is the data protection officer of Callpoint AG, see also Section 1.

For data protection concerns regarding qualified electronic signatures, please contact the data protection officer of Swisscom Trust Services AG, see also Section 1.

The data processing described here is carried out by

ti&m AG
Buckhauserstrasse 24
8048 Zürich
Switzerland
Tel.: 044 497 75 00
E-Mail: marketing@ti8m.ch

In case of doubt, or if you have concerns that specifically relate to data processing by ti&m, you can communicate them to us at the following contact address (this is also the address of our data protection officer under Art. 37 DSGVO):

ti&m AG
Stefan Bühlmann
Buckhauserstrasse 24
8048 Zürich
Switzerland
E-Mail: dpoffice@ti8m.ch

Our representative in the EEA under Art. 27 DSGVO is:

ti&m GmbH
Markus Sell
Schaumainkai 91
60596 Frankfurt am Main
Germany
E-Mail: dpoffice@ti8m.ch

3. Collection and processing of personal data

We only process personal data that you provide to us in the course of online identification or video identification. These are:

On identification documents, the following elements are extracted (if available):

- first name
- surname
- date of birth
- nationality
- expiration date
- photo
- identity document number
- signature
- gender
- identity document type
- MRZ (Machine Readable Zone)

Identity documents may contain other elements (for example, size) that are ignored. In the case of biometric ID documents and identification via mobile app, the above data (except the MRZ) can be read from the NFC chip using NFC (Near Field Communication).

During the identification process

- photos of the ID document (front and back)
- photos of you
- either an audio recording or a video recording

are created and stored, and your

- contact information (e-mail, mobile number) and
- address will be requested

During online identification, Swiss addresses are checked using the Swiss Post's address check service and German addresses are checked using the German Post's services.

If an address is not available in the register of the respective post office

- a utility bill, e.g. an electricity bill

can be uploaded.

In connection with the use of our website and app, additional data may be collected, such as IP address, MAC address, operating system of your device, information about your device and settings, the browser you use and its 'user-agent', cookies, date and time of visit, pages and content viewed, functions used, website from which the access occurred, location information and the amount of data transferred.

4. Purposes of data processing and legal basis

We use the personal data we collect to identify the persons to the controller. In the case of banks and insurance companies, this is done on the basis of [FINMA Circular 2016/7 "Video and online identification"](#).

The requirements of the ETSI standard (TS 119 461 V1.1.1 of 2021-07) apply for all controllers: https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf.

And in the case of the qualified electronic signature, the "Federal Law on Certification Services in the Field of Electronic Signature and Other Applications of Digital Certificates" <https://www.fedlex.admin.ch/eli/cc/2016/752/de> applies.

By using the identification service, you give us your consent to process your data as described. You may revoke your consent at any time, but this will not affect any data processing that has already taken place.

For the purpose of further development, quality improvement and statistical evaluation of the online and video identification service described here, ti&m AG logs data on individual data calls. This logged data does not contain any personal data and does not enable any persons to be identified.

ti&m does not use the data for any other purpose, not even for advertising, or for market or opinion research.

5. Cookies and user tracking

No cookies or other tracking technologies are used.

6. Data sharing and data transfer abroad

ti&m deletes all data held by it after 30 days at the latest.

We return all data collected during online identification or video identification (see Section 3 "Collection and processing of personal data") to the controller. We do so regardless of whether or not the identification process was successful.

For the creation of the qualified electronic signature, ti&m forwards all collected data to Swisscom.

The controller may be obligated to pass on the recorded data to supervisory or other authorities in order to comply with legal and regulatory requirements.

The controllers are located in Switzerland or the EU. For European controllers, the GDPR applies.

The data will never be transferred to a country without adequate legal data protection and the online identification or video identification service will not be provided to any controller in such a country.

7. Duration of the storage of personal data

If an identification is completed, the data is immediately transferred to the controller and ti&m deletes this personal data afterwards.

If an identification is not completed for a longer period of time, the data collected in the course of this identification will only be accessible to ti&m for a maximum period of 30 days. After this period, the data will be deleted by ti&m. ti&m cannot access your data after this period.

The data will be transferred beforehand to the controller for further processing. How long the controller stores the data depends on their business processes and can be read in their privacy policy or requested from their data protection officer.

The data is also transmitted to Swisscom for the qualified electronic signature. How long Swisscom retains the data is regulated in its data privacy policy.

8. Data security

We take appropriate technical and organizational security measures to protect your personal data from unauthorized access and misuse, such as the issuance of warnings, training, IT and network security solutions, access controls and restrictions, encryption of data carriers and transmissions, pseudonymization.

9. Obligation to provide personal data

As part of the identification process, you must provide the personal data that is required to carry out the identification; as a rule, you do not have a legal obligation to provide us with data. Without this data, however, we will not be able to identify you to the controller. You will then have the opportunity to personally identify yourself to the controller on site.

10. Profiling and automated decision making

For identification purposes, we use partially automated decision making (as regulated in Art. 22 GDPR). We process your personal data in an automated manner with the aim of evaluating certain personal aspects, for example, to check the validity of identification documents. ti&m uses the data exclusively in accordance with Section 4 "Purposes of data processing and legal basis" and for no other purposes.

If an identification is refused by our software, you always have the possibility to identify yourself personally to the controller on site.

11. Rights of the data subject

Within the scope of the data protection law applicable to you (such as in the case of the GDPR), you have the right to information, correction, deletion, the right to restrict data processing and otherwise to object to our data processing as well as to the sharing of your personal data. Please note, however, that we reserve the right to enforce the restrictions provided for by law, for example if we are obliged to retain or process certain data, have an overriding interest in doing so (insofar as we are entitled to invoke this) or require it for the assertion of claims. If you incur costs, you will be informed in advance. We have already informed you about the possibility

of revoking your consent in Section 4. Please note that the exercise of these rights may conflict with contractual agreements and may have consequences such as the premature termination of the contract with the controller or cost implications.

The exercise of such rights usually requires that you clearly prove your identity (e.g. by a copy of your identity card, if your identity is not clear or cannot be verified).

In order to assert your rights, you can contact the data protection officers indicated in Section 2.

In addition, every data subject has the right to enforce his or her claims in court or to file a complaint with the competent data protection authority. The competent data protection authority in Switzerland is the Federal Data Protection and Information Commissioner (<http://www.edoeb.admin.ch>).

12. Changes

We may amend this data privacy policy at any time without prior notice. The current version published in the app and on our website applies.

* * * * *