

Privacy Policy for Web App and Mobile App

Version 2.0
effective from February 23, 2023



PEAX AG, Landenbergstrasse 39, 6005 Lucerne (“**we**” or “**us**”) offer the web application PEAX (“**web app**”) and mobile application PEAX (“**mobile app**”) and also operate these apps. Where the web app and the mobile app are indicated, this privacy policy will refer to the **app**. We are thus responsible for the collection, processing and use of your personal data and the reconciliation of data processing with the applicable data protection laws.

You can reach our Data Protection Officer using the following contact information:

PEAX AG
Landenbergstrasse 39
6005 Lucerne
Switzerland
Email: info@peax.ch

In the app, we enable you to call up and display your digital Post-box as a user either of a private or of a business account. If we do not explicitly indicate that a function is reserved for a private or business account, the function can be used by both account types, with the following functions in particular enabled:

- Mail redirecting management;
- document receipt;
- document scanning and uploading;
- document filing and processing;
- invoice payment;
- contact management;
- viewing the PEAX transaction account (accounting preview, account statement);
- account management.

When you use the app, your personal data is processed by us. Personal data includes all information which refers to an identified or identifiable person. Because protecting your privacy is important to us, we would like to provide details below about which personal data we process when you use our app and how we deal with this data.

Your trust is important to us. As a matter of course, we therefore observe the legal provisions of the Federal Act on Data Protection (**FADP**), the Ordinance to the Federal Act on Data Protection (**OFADP** and **ODP**), the Telecommunications Act (**TCA**) and other applicable provisions of Swiss or EU data protection law, if any.

You can call up the privacy policy at any time on our apps under the menu entry “**Privacy policy**”.

Data processing in conjunction with our apps

1. Which information is collected when you download the mobile app on a mobile device?

When you download the mobile app, certain required information is transmitted to the App Store (such as Google Play or Apple App Store) you have selected. In particular, user name, email address, the customer number of your account, the time of download, payment information as well as the individual device identification number can be processed. This data is processed exclusively by the respective App Store and is outside of our sphere of influence.

2. Which data is collected when I create an account and register myself on the apps?

When you create a profile or log in, we use your access data to grant you access to your account and to manage it accordingly. The mandatory information required is:

- email address;
- details of scope of functions;
- title;
- first name;
- last name;
- address;
- date of birth;
- gender;
- payment information

Mandatory data is marked with an asterisk during registration. If you do not provide this data, you will not be able to create an account. You will also receive a PEAX ID and a Peaxbox email address.

In addition, you can enter optional information, such as your phone number, marital status, place of birth, home town, nationality, native language, social insurance number or a profile picture.

We use the mandatory data to create a profile, to authenticate you at login and to follow up on requests to reset your password. From ID levels 1 and 2, we also use this mandatory data to identify you as a person and your postal address. This data thus needs to be processed in order to carry out pre-contractual and contractual measures and is in our legitimate interest. We also require the mandatory profile information to provide our services. This data thus needs to be processed in order to carry out pre-contractual and contractual measures.

We use optional information to display and utilise it according to the settings you have made in the app. This additional optional data is only processed if you enter it and processing is therefore based on your consent.

3. Which authorisations are required for using the mobile app?

The mobile app also requires the following authorisations:

- Internet access: This is required to save your entries on our server.
- Camera access: This is required so that you can take photos of your documents and save them in the app as well as on our servers.
- Upload and download directories as well as photo and media library: This access is required to upload and download documents in the app.

This data must be processed in order to meet pre-contractual and contractual obligations as well as to use the mobile app. We can pass on this data to third parties to read information (also known as “capturing” on our behalf).

4. Is information collected automatically when you use the mobile app?

As part of your usage of the mobile app, we collect certain data automatically, which is required for using the app. In particular, this includes:

- internal device ID;
- version of your operating system;
- time of access.

This data is collected and processed for the purpose of enabling the use of our mobile app (connection setup), to guarantee system security and stability on a permanent basis and to enable our offer to be optimised, as well as for internal statistical purposes. This is our legitimate interest in processing the data.

In the event of attacks on the network infrastructure or other prohibited or abusive usages, the internal device ID will also be evaluated together with the other data for clarification and defence purposes, and might also be used against the respective users in criminal proceedings for identification purposes, as well as in civil and criminal action. The processing of this information lies in our legitimate interest in preventing unauthorised access in future and improving our system stability accordingly. If we do not require the data for management procedures or a judicial, administrative or criminal proceeding and forward it in this context, this data is not passed on.

5. Which information is collected when you call up the web app?

When you call up our web app, our servers temporarily store every access in a log file. The following technical data is then collected without any input on your part, as is always the case in any connection with a web server, and stored by us until it is automatically deleted:

- the IP address of the requesting device;
- the geographical location of the IP address;
- the name of the owner of the IP address area (usually your Internet access provider);
- the date and time of access;
- the website from which access was made (referrer URL), possibly with the search term used;
- the name and URL of the calling file;
- the status code (such as error message);
- the operating system of your computer;
- the browser you are using (type, version and language);
- the transmission protocol you are using (such as HTTP / 1.1);
- if necessary, your user name from a registration/authentication.

This data is collected and processed for the purpose of enabling the use of the web app (connection setup), to guarantee system security and stability on a permanent basis and to enable our offer to be optimised, as well as for internal statistical purposes. This is also our legitimate interest in processing the data.

In the event of attacks on the network infrastructure or other prohibited or abusive usages, the IP address will also be evaluated together with the other data for clarification and defence purposes, and might also be used against the respective users in criminal proceedings for identification purposes, as well as in civil and criminal action. We have a legitimate interest in such data processing, in order to prevent unauthorised access in the future and to improve our system stability accordingly. If we do not require the data for management procedures or a judicial, administrative or criminal proceeding and forward it in this context, this data is not passed on.

6. Which data is collected when the apps are used?

When you use the apps, you can also manage and process various information on the profile data. In particular, this information collects personal data which we obtain from you directly (such as photo, change of address, bank data) as well as data which we receive via interfaces. The processed data depends on the function used. We process the data which is necessary to offer you the functions described below for the purpose of meeting our contractual obligations. We will process all data that you have provided voluntarily (for example, by uploading documents) based on your consent. You can revoke this consent at any time by modifying the respective data in the app. Whenever your data is processed, PEAX is particularly aware of the sensitivity of this data and, in particular, your documents. Access possibilities are therefore limited to the necessary employees and the data is only processed for the purpose of providing the contractual services or for purposes to which you have explicitly agreed. Unless we have stated otherwise below, we will not pass this data on to third parties.

With your private account, you can use all the functions listed below which are activated for your account. In the business accounts, the functions which you can use also depend on which role you have been assigned. Accordingly, the functions available to you for use might be more or less comprehensive.

a. Mail redirecting management

You can organise Mail redirecting directly in the app if you have the appropriate PEAX ID level as well as the respective subscription. In particular, we need address data for this purpose. We work together with Swiss Post AG (Post) as regards Mail redirecting and in this context can also disclose your data to the Post and its support staff.

b. Document receipt

You can receive documents in the app via Mail redirecting, Peaxbox email address or by forwarding. In addition to information on senders and recipients, we can also receive data on the received documents in this manner. You can of course delete the received documents again at any time.

c. Document scanning and uploading

Various documents (such as receipts, vouchers or till receipts) can be uploaded or scanned in the app. In addition to information on the users performing the actions, we can also receive data on the received documents in this manner. You can of course delete the received documents again at any time.

d. Document processing

You can process documents stored in the app, which enables us to receive data on the processing as well as, if necessary, the document.

e. Invoice payment

You can upload invoices and delete them again later in the app. In addition, you can also pay invoices. To pay invoices via the app, we need the account information of the invoicing party. This is usually the account number, the contact data of the invoicing party, the amount and the date.

To be able to offer this function, we work together with a Swiss bank and use an interface from this bank for payment processing. Accordingly, we can only enable communication with banks in the network of our interface provider. As part of this cooperation, we can forward your data and the data of the invoicing party to the bank.

f. Contact management

You can manage contacts in the app and enter and/or delete various contacts. The respective contact information is required for this purpose. You can enter and/or delete various organisations in the app. Data on the organisations to be entered is required for this purpose (such as contact data, customer numbers and other optional information).

**g. Viewing the PEAX transaction account
(accounting preview, account statement)**

You can enter information on your bank or on a business account of the bank of the business account holder in the app. Bank data is required for this purpose. In particular, this is the IBAN, the name of the bank, the branch, the clearing number and the name of the account. You can also make optional entries (such as the account manager). In order to provide this function, we also need to collect information on the economic beneficiaries. We do this using standardised forms which request the information required by law.

The app can also be used to view the account statement or the posting preview of the PEAX transaction account. This enables the data visible in the account statement to be processed.

h. Account management

In addition, you can manage your account at any time in the app and add or delete data in it. We need the account data stored in order to be able to provide you with our functions. In addition, you can enter further optional data.

As a business account holder, you can also invite new users, assign them particular roles and establish a link to the business account.

7. Cookies and application data

Cookies help in many ways to make your visit to our web app easier, more enjoyable and more useful. Cookies are information files which automatically store your web browser on your computer hard drive. Application data consists of information files that are stored locally on your device to enable convenient and expedient use on a permanent basis when you use the mobile apps.

For example, we use these cookies to temporarily store your chosen services and entries when filling out a form in our web app, so that you do not have to repeat the entries when you call up another sub-page. Cookies might also be used to identify you as a registered user after you have registered on the website, so that you will not have to log in again when you call up another sub-page.

Most Internet browsers accept cookies automatically. However, you can configure your browser such that no cookies are stored on your computer or a note always appears when you receive a new cookie.

Deactivating cookies might mean that you cannot use all the functions in our web app.

When you call up our apps, we or third parties save the following user-specific information in particular:

For the web app:

Cookie	Description	Purpose	Storage duration
ai_session	Identifier for application insights	Is used to group telemetric data for each user session.	Only during active session
ai_user	User identification in logging	All requests will be supplemented with this user identification in order to assign them to this "user" in logging.	Only during active session
PEAX_LANG	Portal language	Enables portal to be displayed in the language previously selected	12 months

Mobile app for Android:

Application data	Description	Purpose	Storage location	Storage duration
ENCRYPTED_EMAIL	Encrypted user email address	Use for biometric authentication	Local device of user	As long as the app is installed or the app data is not deleted
ENCRYPTED_PASSWORD	Encrypted user password	Use for biometric authentication	Local device of user	As long as the app is installed or the app data is not deleted
CURRENT_USING_SERVER	Current environment (api) of the application	Enables connection to be established between the local app and the mobile app.	Local device of user	As long as the app is installed or the app data is not deleted
PORTAL_LANG	Storage of the current application language	Enables the app to be used in the language previously selected.	Local device of user	As long as the app is installed or the app data is not deleted
CHANGED_LANGUAGE	Marker for UX Refresh	Technical marker if you choose a different language.	Local device of user	As long as the app is installed or the app data is not deleted
DEVICE_UUID	Device identifier	Enables the device used to be identified.	Local device of user	As long as the app is installed or the app data is not deleted
PRIVATE_ACCOUNT_ID	Account identifier	To identify the user	Local device of user	Only during active session
CURRENT_SELECTED_ACCOUNT_ID	Description of account currently used	Enables connection with the correct account.	Local device of user	Only during active session
LAST_LOGIN_EMAIL	Last email login	Last logged in email address will be displayed, so that you do not have to enter it again.	Local device of user	As long as the app is installed or the app data is not deleted

Mobile app for iOS:

Application Data	Description	Purpose	Storage duration
checkInProcessed_Finished	Stores whether the user has completed onboarding	Ensures that the login process only has to run through once.	As long as the app is installed or the app data is not deleted
emailText	User name or email address	User name or email address is displayed so that you do not have to enter it again as well as for use in biometric authentication.	As long as the app is installed or the app data is not deleted
passwordText	User password	Use for biometric authentication	As long as the app is installed or the app data is not deleted
accountID	PEAX ID	To identify the user	As long as the app is installed or the app data is not deleted
private_user_profile	Account identifier	To identify the user	Only during active session
current_user_profile	Description of account currently used	Enables connection with the correct account.	Only during active session
device_tokens	Device identifier	Enables the device used to be identified.	Only during active session
sealed_credentials	Login data	Enables use of the login data protected in iOS for login.	Only during active session
session_data	Status of app use	Enables continued use of the app at the same place, e.g. after the app ran in the background.	Only during active session

Storage and exchange of data with third parties

8. Will this data be stored or linked?

We host the app on Microsoft Azure. Our contractual partner is Microsoft Schweiz GmbH (Zurich Airport, The Circle 02, 8058 Zurich), which is a company of the Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA (together **Microsoft**). As Microsoft operates globally, legal or regulatory obligations may require personal data to be transmitted to countries outside the country where the personal data was originally collected. Because Microsoft is headquartered in the United States, the laws of the United States may require Microsoft to routinely transmit personal data collected in other countries to the United States for processing. With data transmissions to the USA, Microsoft applies the terms and conditions which are defined in the EU standard contract clauses for the collection, use, storage and transmission of personal data.

The services will be provided from Switzerland, Europe and Australia. We base the processing of this data in the software on our legitimate interest in customer-friendly and efficient customer data management.

9. How long will my data be stored?

We only store personal data for as long as is necessary to enable the processing mentioned above based on the principles described. We retain contract data for a longer period of time, as this is required by statutory retention requirements. Retention requirements which oblige us to retain data are derived from accounting regulations, civil law and tax law. According to these regulations, business communications, concluded contracts and accounting records must be retained for up to 10 years. If we no longer need this data to perform the services for you, the data will be blocked. Your data will be deleted after 10 years since the end of the relevant fiscal year.

10. Will my data be forwarded to other third parties?

We will only pass your personal data on to third parties if you have given your express consent, a legal obligation exists to do so or this is necessary to enforce our rights, in particular to enforce claims arising from the contractual relationship. We also give your data to third parties if this is required for using the app and contract processing. In addition to the third parties mentioned in the privacy policy, these are:

Recipient category	Purpose of data transfer	Location	Guarantees
Partner subscription management and billing	Automation of accounting processes	USA	EU standard contract clauses and data protection impact assessment for data transmission
Scanning partners	Scanning of received shipments and delivery to portal	Switzerland	Legislation guarantees appropriate data protection
Capturing partners	Analysis and readout of relevant document contents for the identification and filing of document types, preparation of payment execution as well as full text search in the portal	Switzerland	Legislation guarantees appropriate data protection
Partners for technical support	Provision of technical support in services and tools by third parties	USA, Australia, Europe	EU standard contract clauses and data protection impact assessment for data transmission and legislation guarantee appropriate data protection according to FDPIC
Web page monitoring and web service monitoring providers	Ensuring availability and performance of web app and mobile app.	Europe	Legislation guarantees appropriate data protection according to FDPIC
Partners for email dispatch and monitoring	Email marketing and transaction emails of the portal (notifications without personal data contents such as notification on information regarding the existence of a Postbox)	Australia	Legislation guarantees appropriate data protection according to FDPIC
Communication interface providers	SMS dispatch for two-factor authentication	USA	EU standard contract clauses and data protection impact assessment for data transmission

11. Do we send personal data abroad?

We are authorised to also transmit your personal data for the purpose of the data processing described in this privacy policy to third-party companies (contracted service providers) abroad. These companies are committed to data protection to the same extent as we are. If the data protection level in a country does not correspond to the level in Switzerland or in Europe, we will ensure in contractual and technical terms that the protection of your personal data will correspond to that in Switzerland and in the EU at all times.

Do you need to know anything else?

12. You have a right to information, rectification, deletion and restriction of processing as well as to data transferability

You have the right to receive information upon request regarding the personal data you have stored with us. You also have the right to the correction of incorrect data and the right to delete your personal data, if this does not conflict with any legal obligations to retain the data or an authorisation that allows us to process the data. In the event of disagreement, you also have the right to have a notice of objection made.

In addition, you have the right to ask us to return the data that you have submitted to us (right to data portability). Upon request, we will also forward the data to a third party of your choice. You have the right to receive the data in a common file format.

You can reach us at the email address support@peax.ch for the purposes mentioned above. In order to process your request, we can, at our own discretion, require proof of identity.

The aforementioned rights are dependent on the respective applicable data protection legislation and can therefore be either more limited or more comprehensive.

13. Is your data safe with us?

We use appropriate technical and organisational security measures to protect the personal data you have stored with us against manipulation, partial or complete loss and against unauthorised access by third parties. Our security measures are being continuously improved in line with technological development.

You should always treat your access data as confidential and log out once you have concluded your communication with us, in particular, if you use your computer, tablet or smartphone jointly with others.

We also take internal data protection very seriously. Our employees and the service companies we commission are obliged by us to maintain confidentiality and to comply with the provisions of data protection law.

14. Does the same protection exist if data is transmitted to the USA?

For the sake of completeness, we draw the attention of users resident in or with headquarters in Switzerland to the fact that in the USA, surveillance measures of the US authorities are in place which generally allow the storage of all personal data of all persons whose data has been transmitted from Switzerland to the USA. This is performed without differentiation, restriction or exception based on the pursued objective and without an objective criterion which enables the US authorities' access to the data and its subsequent use to be restricted to very specific, strictly limited purposes, which are capable of justifying the interference associated with both access to and use of this data. We also draw attention to the fact that no legal remedies are available in the USA for the persons concerned from Switzerland which enable you to receive access to the data concerning you and to enforce its correction or deletion, and that there is no effective legal protection against general access rights by US authorities. We explicitly draw your attention to this legal and factual situation, in order to enable you to make an appropriately informed decision regarding the consent to the use of your data.

We draw the attention of users resident in a member state of the EU or in Switzerland to the fact that the USA, from the perspective of the European Union – among other things, based on the issues mentioned in this section – does not have a sufficient level of data protection. Insofar as we have explained in this privacy policy that recipients of data (such as Microsoft) have their headquarters in the USA, we will ensure through contractual arrangements with these companies or other guarantees that your data at our partners is protected at an appropriate level.

15. Can you complain about us?

You have the right to lodge a complaint against us at any time at support@peax.ch or at a responsible data protection supervisory authority.

16. Which law do we apply? And where is this law applied?

This privacy policy and the contracts which are concluded based on or in connection with this privacy policy are subject to Swiss law, unless the law of another country is mandatorily applicable. The place of jurisdiction is at the headquarters of PEAX AG, unless another place of jurisdiction is mandatorily specified.

17. Can this declaration be changed?

If individual parts of this data policy become ineffective, this does not affect the validity of the rest of the privacy policy. The ineffective part of the privacy policy must be replaced with a section that comes closest to the economically intended purpose of the invalid part.

Due to the further development of our apps and offers or due to changes in legislation or official requirements, it might become necessary to change this privacy policy. The current privacy policy is accessible on our apps.

18. Do you have any questions on data protection?

Then get in touch!

This page was last changed on February 23, 2023. If you have any questions or comments on our legal notices or our privacy policy, please contact us at support@peax.ch.

Our postal address is:

PEAX AG, Landenbergstrasse 39, 6005 Lucerne, Switzerland