

TOKEN
TEN

Web-App Privacy & Cookie Notice

VERSION 2.0 August 2026

TOKEN

1. Introduction

Token GmbH and Token.io Ltd (hereinafter referred to as “Token.io”, “we”, “our”, “us”) is always aware of the importance of the data entrusted to us.

The responsible handling, confidentiality and protection of our user’s (“you”, “your”) data is therefore of particular importance to us.

The Processing of your personal data is carried out exclusively within the framework of the statutory provisions, the applicable data protection law and this Web-App Privacy & Cookie Notice (“Privacy Notice”).

This Privacy Notice relates to the use of the Token.io web-application.

2. Purpose of this Privacy & Cookie Notice

This privacy and cookie notice aims to give you information on how Token.io collects and processes your personal data when you use our Web-App service.

We ask you take note of this privacy and cookie notice alongside any other policies published on our website, which outlines the data we collect about you, so you’re fully informed and aware of how and why we are using your data.

This privacy and cookie notice supports and supplements other notices published on our website and is not intended to override them.

3. The subject of data protection

The subject of data protection is personal data. Individual specifications about the personal or objective relationships of a defined or definable natural person. Personal data is therefore information that can be used to draw conclusions about an identified or identifiable natural person.

In principle, all information about which a personal reference can be established also qualifies personal data. For example, a person’s name, address, e-mail address, telephone

number, personnel number, vehicle registration number plate, appearance or walk are personal data.

‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

4. Controller / Processor

For most of our services, Token.io acts as a Data Processor: the information we process is instructed by your bank or the merchant, who act as the Data Controller and define how Token.io processes this information under our contractual agreements with them. They should outline this to you in their own privacy policy or notice.

If you use our cVRP (commercial Variable Recurring Payments) service, Token.io may instead act as an independent Data Controller in respect of personal data we share with an ASPSP Participant (your bank) or our clients who make cVRP available to you as a payment option — for example, to set up, execute or manage your mandate. This may also apply to personal data we share with UK Payments Initiative Limited (as operator of the cVRP scheme) or other ASPSP Participants, where necessary to investigate and resolve a dispute about a cVRP mandate or transaction (see Section 7 below).

Please see the [Privacy Policy](#) on our website for more information and contact your bank / the merchant to view their privacy policy.

5. What personal information do we collect from our users?

We do our best to minimise the amount of Personal Information that we collect from our Token.io users.

Our processing of your personal data is limited to the following: First name, Last name, Mobile Phone, Email, Passcode, Face ID, account details, transaction details etc.

We process this information only for the purposes of establishing and administering your account, facilitating a payment request with your selected payment service or financial institution, communicating with you when you ask us for support, or if you report a bug or other error.

If you use our cVRP (commercial Variable Recurring Payments) service, we may also process: details of your cVRP Mandate and the consent you have given for it; your Consent Parameters (such as the recipient, payment frequency and maximum amount you have authorised); details of your cVRP payment initiation and cancellation requests; and where relevant, information about complaints you raise regarding a Biller's use of cVRP as a payment method (this does not include complaints about the goods or services themselves), which may also be used to help identify practices that could be harmful to other Payers or to the cVRP scheme.

We process this cVRP-related information to establish and manage your cVRP mandate and the payments made under it; to act on your instructions when you cancel or revoke a mandate; to investigate and resolve complaints or disputes relating to cVRP and to meet our record-keeping obligations under the cVRP scheme rules.

We will also procure that our clients (or, where applicable, their own merchants) give you a facility to view and revoke your cVRP mandates directly; monitor your mandates for extended inactivity; notify you before a mandate that has been dormant for 13 consecutive months is cancelled; notify you before a mandate is due to expire; and issue any pre-notifications required before a payment is taken.

TOKEN

6. Legal Basis (UK and EU General Data Protection Regulations)

We rely upon the legal basis of Art. 6 Para. 1 lit. b GDPR (EU) when we process your personal data for the **purposes of acting as an infrastructure provider for open banking and allowing you to carry out the transaction from the merchant site.**

The processing is necessary for the performance of a contract (or service) to which you are a party or in order to take steps at your request prior to entering into a service.

[Our terms and conditions of service can be found here.](#)

We may also use your personal information to analyse performance, fix errors, and improve the usability and effectiveness of Token.io services.

We rely on Art. 6 Para. 1 lit. f GDPR (EU) Legitimate Interests when we process your personal data for the **purposes of analysis and maintenance of our system and application access data**, internet and electronic network activity information, including your Internet protocol (IP) address used to connect your computer or mobile device to the Internet. We use your personal information to enable Token.io service metrics (e.g., the occurrences of technical errors, your interactions with service features and content, your settings preferences, records of any contractual agreements between yourself and Token.io and to provide troubleshooting, improve Token.io Services).

For information on how Token.io safeguards personal data transferred outside the EEA or UK, including the mechanisms used and a list of our sub-processors, please see Section 8 (Third Party Sub-Processors), Section 9 (cVRP Scheme Participants) and Section 10 (International Transfers) of our [Privacy Policy](#).

7. Will we share your personal data with third parties?

Information about you as our users is an important part of our business and we do not sell our users' personal information to others.

We transfer your personal data via our Service to your chosen payment service providers (e.g. our client Banks and financial institutions) where we act as a data processor on behalf of those organisations under contract to them.

Once a payment request is initiated by you, the recipient financial institution is thereafter the data controller for all interactions relating to that payment and you are advised to review the privacy policies of the institutions you nominate.

In connection with Token's operation of its business, where we rely on various third-party products and services, these third party services providers only have access to the minimum personal information necessary to perform their service to us and may not use it for any other purposes. Furthermore, they must process the personal information in accordance with our contractual agreements and only as permitted by applicable data protections laws.

If you use our cVRP (commercial Variable Recurring Payments) service, we may share personal data relating to your cVRP mandate or transactions with:

- **ASPSP Participant (your bank)**, as an independent controller, as part of the normal operation of the cVRP scheme — for example, to set up, execute, or manage your mandate;
- **our clients** who make cVRP available to you as a payment option, whether or not they are themselves payment initiation providers, as part of the normal operation of the cVRP scheme — for example, so they can confirm your mandate and receive the payments you've authorised.

We may also share limited, and where possible redacted, personal data with:

- **UK Payments Initiative Limited ("UKPI")**, as the operator of the cVRP payment scheme;
- **other ASPSP Participants** in the cVRP scheme,

where necessary to investigate and resolve an issue or dispute relating to a cVRP mandate or transaction.

ASPSP Participant (your bank), UKPI, and other ASPSP Participants in the cVRP scheme each act as an independent controller of any personal data shared with them for these purposes. Our clients' role in relation to any personal data we share with them depends on our contractual arrangements with them, as set out in their own terms or privacy notices.

8. Business transfers

As we continue to develop our business, we might sell or buy other businesses or services. In such transactions, user information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing privacy notice (unless, of course, the user consents otherwise). Also, in the unlikely event that Token.io, or substantially all of its assets are acquired, your user account information will be one of the transferred assets.

We will share personal information outside of Token.io if we have a reasonable belief that access, use, preservation, or disclosure of the information is reasonably necessary to comply with any applicable law, regulation, legal process, or enforceable governmental request; to cooperate with law enforcement; to enforce or apply our Terms and Conditions of Use and other agreements; or to protect the rights, property, or safety of Token.io employees, our users, or others.

9. YOUR RIGHTS WITH RESPECT TO THE PROCESSING OF PERSONAL DATA

You are entitled (under the conditions, and subject to the exceptions, set out in applicable law) to:

- Be informed about the processing of personal information (this notice)
- Request Access to the personal information we process about you: You can request access to the information we have collected from you, free of charge.
- Request a rectification of your personal data: If you believe that the information we have collected is incorrect or incomplete, you may contact us so we can update it and keep your data accurate.
- Object to the processing of your personal data: you may request that we no longer process your personal data.
- Request to erase your personal data: you may request the erasure of your personal data, including where such personal data would no longer be necessary to achieve the purposes for which it was collected.
- Request the restriction of the processing of your personal data: you may request that Token.io only processes your personal data in limited circumstances, including with your consent.

You can do this or request to exercise any of your rights below by contacting us at:

Privacy@token.io

To comply with your request, we may ask you to verify your identity.

10. Data Retention

Please note that even If you delete your Token.io App or data from your mobile application, uninstall Token.io mobile application from your device, or request that your

TOKEN

information be deleted, we still may retain some information that you have provided to comply with the laws and regulations to which Token.io is subject.

It is a legal requirement for financial institutions to retain financial data for 7 years in the UK and 10 years in Europe.

For cVRP mandates specifically, we retain your mandate, consent and consent-parameter records for at least 6 years. This period starts from whichever happens last — your final payment under that mandate or the date it expires or is cancelled — and runs from that later date. This is consistent with our other financial record-keeping obligations above.

Other cVRP-related records — such as details of your payment initiation and cancellation requests, and any complaints information — are retained for at least 6 years from the date the relevant record was created.

If you have any question or objection as to how we collect and process your personal information, please contact us.

11. Data Security

We are committed to making sure your information is protected in accordance with applicable laws and our data privacy policies. We have selected third-party vendors that help us keep your Personal Information safe. We maintain physical, electronic and procedural safeguards in connection with the collection, storage and disclosure of your personal information and maintain formal certification to internationally recognised standards for information security management.

12. Children

We are especially sensitive about children's information. Our Services are not targeted towards children, and our users must be at least eighteen (18) years old to use our services. We do not knowingly collect personal information from anyone under this age. If you are a parent or legal guardian and believe a minor has provided us with personal information, please contact us at Privacy@token.io.

13. Conditions of use, notices, changes and updates to Privacy Notice

If you choose to use Token.io services your use and any dispute over privacy is subject to this Notice and our Terms and Conditions of Use. If you have any concerns about privacy at Token.io please contact us with a complete description, and we will try to resolve it. You also have the right to contact your local Data Protection Authority. We reserve the right to update and revise this Privacy Policy at any time. We occasionally review this Privacy Notice to make sure it complies with applicable laws and conforms to changes in our business. If we do revise this Privacy Notice, we will update the "Effective Date" at the top of this page so that you can tell if it has changed since your last visit and will do our best to notify you. Please review this Privacy Notice regularly to ensure that you are aware of its terms. Any use of the Token.io App after an amendment to our Privacy Notice constitutes your acceptance to the revised or amended terms.

14. Cookies

- a. A cookie is a small bit of information that a website stores on your computer and when using the Token.io Web-App, cookies are required in order for the webapp to function. When we refer to cookies we are also referring to unique identifiers used

to identify a device and authenticate the realness of the transaction. For the purpose of this section we will refer to cookies and/or identifiers as 'identifiers'.

- b. The identifiers used on the Token.io Web-app are locally stored on your device which you have the ability to remove at any time and Token.io do not have access to these identifiers.
- c. The Token.io Web-App only uses 'necessary' cookies that are crucial for the basic functions of the webapp and the webapp will not work in its intended way without them.
- d. These cookies do not store any personally identifiable data. These cookies are opt-out. You can find guidance below on how to remove these:
 - i. [Google Chrome](#)
 - ii. [Microsoft Edge](#)
 - iii. [Firefox](#)
 - iv. [Safari](#)

[Deactivation of identifiers may lead to the webapp being unusable.](#)

e. The Cookies / Identifiers

Cookie Identifier	Purpose	Duration
recentBanks	list of bankIds to identify recently selected banks (by this PSU)	Until user clears cache
deviceId	random string to uniquely identify the device.	Until user clears cache
reduxState	contains details of Token.io request payload.	Until user clears cache
popup_id	unique string to identify the popup.	Until user clears cache
Version	random number.	Until user clears cache
bank	bank details.	Until user clears cache

TOKEN

15. Your rights in relation to Cookies

Regulation 6 of The Privacy and Electronic Communications Directive 2003 (PECR) outlines that Token.io must:

- Provide you with clear and comprehensive information about the purpose and storage of information. This is covered by sections 14 (b) and 14 (e) of this policy.
- Give you the opportunity to refuse access to this information. Section 14 (d) gives you an overview on how to remove these cookies from your device.
- In addition, Token.io aligns with Art.6 Para.1 Lit.(B) of GDPR regulation for lawfulness of processing as a combination of these identifiers may pertain to the processing of personal data.

If you have any questions, please contact our data protection officer at Privacy@token.io. In addition, the identifiers used on the webapp are strictly necessary for carrying out the function of the web-app and therefore under Regulation 6 paragraph 4 (a) we are exempt from obtaining consent for this reason.