

General Privacy Policy

The following general privacy policy (the 'Policy') will give you an overview of how we process your personal data and your rights under data privacy law. Which data are processed and how they are used depends on which services are utilized. Whenever data processing deviates from this information for isolated cases, we will give you separate information as part of the products or services in question.

In particular, the following data protection information exists in addition to the Policy:

- [Cookie Policy](#)

1 Controller for the data processing

The controller is:

Bank für Tirol und Vorarlberg Aktiengesellschaft
Stadtforum 1, 6020 Innsbruck

T +43 505 333 – 0

E info@btv.at

'BTV', 'we', or 'us').

Contact info for the data protection officer:

E datenschutz@btv.at
by post via the BTV

2 We process the following data

We process the personal data that you or a third party you delegate give us as part of our business relationship. If necessary for rendering our service, we also process personal data that we have permissibly received from commissioned service providers (commissioned processors in accordance with Art. 28 GDPR), distribution partners, credit agencies, debtor registers (such as CRIF GmbH, KSV1870), or publicly accessible sources (such as the company register, land register, register of associations, the media, and the internet).

Relevant personal data include your personal details (name, address, contact data, date and place of birth, citizenship, social security number, familial status, number of children, professional information), legitimation data (such as ID data), and authentication data (such as a signature sample and authorised user/customer number). They can also include order data (such as payment orders), data arising from the fulfilment of our contract obligations (such as sales data in payment transactions), information concerning your financial situation (such as scoring data, rating data, and other data on your creditworthiness), advertising and sales data, documentation data (such as a consultation record), register data, image and sound data (such as video and telephone recordings), data concerning electronic business transactions (such as apps, cookies, and IP addresses), and other data that are comparable with the aforementioned categories.

General Privacy Policy

3 We process your data for the following purposes

We process personal data in compliance with the relevant data privacy regulations, including but not limited to the European General Data Protection Regulation (GDPR) and the Austrian Data Privacy Act (*Datenschutzgesetz, DSG*).

3.1 To meet contractual obligations or perform precontractual measures (Art. 6 (1) (b) GDPR)

We 'process' personal data (as defined by Art. 4(2) GDPR) so we can execute banking transactions and render financial services as part of performing our contracts with you, or to perform precontractual measures on request. The purpose of the data processing is primarily based on the specific product (such as an account, loan, securities, savings deposits, saving with a building society, or mediation) and can include needs analyses, consultation, asset management and asset consultancy, and the execution of transactions or to execute your orders (such as payment and securities orders), among other things.

3.2 To meet statutory requirements (Art. 6 (1) (c) GDPR)

Personal data might need to be processed due to various statutory obligations (such as the Banking Act, Financial Markets Anti-Money Laundering Act, and Securities Supervision Act 2018) or regulatory requirements (such as the European Central Bank, the European Banking Authority, the Austrian National Bank, and the Financial Market Authority) to which we are subject as a bank. Data are processed so we can check creditworthiness, identity, and age; prevent fraud and money laundering; meet control and reporting obligations under tax law; and assess and control our risks, among other reasons.

3.3 Based on your consent (Art. 6 (1) (a) GDPR)

If you've given us your consent to process your personal data (to receive an electronic newsletter, for promotional activities, etc.), the data will be processed to the extent entailed in the consent and only for the purpose specified in the consent. Once you have granted consent, you may withdraw it at any time with effect for the future. Withdrawing consent will not affect the lawfulness of the data processing that was performed before the withdrawal.

3.4 To protect legitimate interests (Art. 6 (1) (f) GDPR)

We will continue processing your data after the contract has been fulfilled if we must do so to protect our legitimate interests or those of third parties. For example:

- Consulting and exchanging data with credit agencies (such as KSV1870 Holding AG, CRIF GmbH) to determine credit risks or default risks;
- Testing and optimizing procedures for a needs analysis and contacting the customer directly;
- Advertising or market and opinion research, unless you have objected to the use of your data for those purposes in accordance with Art. 21 GDPR;
- Use of innovative cloud solutions that enable (among other things) video conferences, data rooms, or joint work on a document for the purpose of the collaboration;
- Recording and publishing video and audio conferences if this is necessary to promote the exchange of knowledge, promote the collaboration, or for training purposes;

General Privacy Policy

- Asserting legal claims and defending during legal disputes;
- Guaranteeing our IT security and our IT operations;
- Preventing and clearing up criminal activity;
- Video monitoring to protect the householder's rights, to collect evidence in the event of criminal activity, or to verify disposals and deposits (at ATMs, for example);
- Measures for building and facility safety (such as physical access controls);
- Measures for business management and to enhance services and products;
- Measures to manage risk in the group

3.5 BTV website

When our website is visited, we collect and store data that you disclose to us voluntarily during contact requests, applications, or newsletter subscriptions (such as your email address, first and last names, telephone number, and inquiry, and the documents you attach).

And the access to our website is logged. To that end, each part of your IP address is stored that might permit conclusions to be drawn about the user's country. We also use cookies and other technology on our website (see [Cookie Policy](#)). If you visit the website www.btv.at, we also store the length of your visit, lists of search terms, your country and browser, the time of your visit, screen or display resolution, visitor statistics, and the pages you call up.

3.6 Customer portal (meineBTV)

With the customer portal (meineBTV), you can access the server of BTV's internet banking in accordance with the underlying terms of business. You will log in and identify yourself using the agreed access data.

The access of the server of BTV's internet banking will be logged for evidentiary purposes. The banking / authorised user number will be used as an identifier for the logging. Moreover, the IP address and the data that a user browser includes in a transmission as standard (user agent) will be stored.

3.7 BTV apps

Our apps allow you to access selected areas of BTV's website and display them in a manner optimized for mobile devices (smartphones, tablets, etc.). The apps also allow you to access BTV's internet banking in accordance with the underlying terms of business. You will log in and identify yourself using the agreed access data. The apps will store your authorised user number if the biometric login is activated. Otherwise, no personal data will be stored in the apps.

3.8 BTV Wallet

The BTV Wallet gives you – in accordance with the underlying terms of use – software for mobile end devices with which you

- install, display, and use your digital payment instruments in the BTV Wallet,
- view the data in the payment transactions with your payment cards and digital payment instruments,
- use value-added services related to mobile payment, and

General Privacy Policy

- store digital images of your physical customer cards and customer retention program in the integrated customer card area and digitally reproduce them. You can also register for customer retention programs, manage them, and use the associated value-added services.

You will log in and identify yourself using the agreed access data. The login and identification will be managed during the use of the BTV Wallet. To use your digital payment instruments (such as digital payment function, ZOIN) and display payment transactions, any retailer data that goes beyond the card data and transaction data (such as retailer name, address, and logo), messages you create to the payment recipient, telephone numbers (yours and the recipient's), any freely selectable alias name (yours and the recipient's), and technical information will be processed.

The data shown on the customer cards presented will be processed so that your customer card can be displayed in the BTV Wallet and reproduced as digital identification (such as a barcode). Moreover, and in connection with using customer retention programs, this firm will process the company's data (such as the company name and/or logo, or the image on the customer cards) in which you have set up a customer account and your Frequent Shopper ID (such as a customer number and/or barcode number). In this regard, the BTV is not the controller for the purposes of the GDPR. We cannot access those data or influence the associated data processing.

4 Categories of recipients

Your data will be provided to the offices and people who need them to meet contractual, statutory, and regulatory obligations, or due to legitimate interests. Furthermore, service providers we commission (processors in accordance with Art. 28 GDPR) and vicarious agents will receive your data if they need them to render the respective service. These are companies in the following categories: credit services, IT services, cloud services, fintech, logistics, print services, telecommunications, collection, advice and consulting, and sales and marketing. All processors and distribution partners must be contractually obligated to protect bank secrecy and not disclose any facts they learn about, and must handle your data confidentially.

As far as passing data on to recipients outside our bank is concerned, we hereby inform you that, as a bank, we are obligated to comply with bank secrecy pursuant to § 38 of the Banking Act and therefore to keep all customer-related information and facts that we learn about in connection with our business relationship a secret. This means we may forward your personal data only if you have expressly released us from bank secrecy in writing in advance, or if statutory, contractual, or regulatory provisions obligate or authorize us to grant information. Under these conditions, recipients of personal data include without limitation:

- Public agencies and institutions (such as the Financial Market Authority, European Central Bank, tax authorities, and law enforcement agencies) if there is a statutory or official obligation;
- Other loan and financial service institutions or comparable institutions that we need to execute the business relationship (for example, depending on the contract, correspondent banks, depository banks, stock exchanges, and credit agencies);
- Companies and agencies for whom you have granted us your consent for data transfer or for whom you have released us from bank secrecy.

General Privacy Policy

5 Transmissions into third countries

Data will be transferred to agencies in countries outside the European Union (known as 'third countries') if this is necessary for the aforementioned purposes, prescribed by law (such as tax declaration obligations), or you have granted us your express consent. If the transmission is not made based on an adequacy decision from the European Commission, we transmit the data based on suitable or reasonable guarantees (such as [Standard Contract Clauses](#)).

6 Retention period

We will process and store your personal data for as long as necessary to meet our contractual and legal obligations. In that regard, we must point out that our business relationship is a continuing obligation that is intended to last for a number of years. If your personal data are no longer needed to meet contractual obligations, they will normally be erased unless they must be processed further temporarily to fulfil retention periods under trade and tax legislation set forth in the Austrian Commercial Code (UGB), the Federal Tax Code (BAO), the Banking Act (BWG), the Financial Markets Anti-Money Laundering Act (FM-GwG), and the Securities Supervision Act 2018 (WAG 2018). The retention or documentation periods specified there last from five to ten years. And the retention period is determined by the statutory limitation periods for the purposes of retaining evidence – under the Austrian General Civil Code (ABGB), these normally last three years, but in certain cases can last up to thirty.

7 Obligation to provide your data

As part of our business relationship, you must provide the personal data that are needed to begin and implement a business relationship and fulfil the associated contractual obligations or that we are obligated by law to collect (due to anti-money laundering regulations, for example). Without those data, we will normally have to refuse to enter into the contract or perform the assignment, or we will no longer be able to perform an existing contract and will have to terminate it at best. However, you are not required to grant your consent to the processing of data that are not relevant for the contract performance or not necessary under statutory or regulatory law.

8 No automated decision-making

Pursuant to Article 22 of the GDPR, we do not generally use fully automated decision-making or profiling to establish and implement the business relationship. If we use those procedures in isolated cases, we will inform you separately if this is prescribed by law.

9 Profiling

We sometimes process your data automatically to assess certain personal aspects (profiling). For example, we use profiling in the following scenarios:

- We are obligated under statutory and regulatory requirements to combat money laundering and the financing of terrorism. Data are evaluated to that end (in payment transactions and other cases).

General Privacy Policy

- We use evaluation instruments so we can purposefully inform and advise you about products. These make it possible for us to use needs-based communication and advertising, including market and opinion research.
- We use scoring as part of assessing your creditworthiness. To that end, the probability that the customer will meet its payment obligations in accordance with the contract is calculated. For example, the calculation can consider income, expenditures, existing liabilities, profession, employer, period of employment, experiences arising from the previous business relationship, repayment of previous loans in accordance with the contract, and information from credit agencies. The scoring is based on a mathematically and statistically acknowledged and proven procedure. The calculated score values support us during the decision-making as part of product deals and are included in the ongoing risk management.

10 Data security

We take protecting your personal data very seriously and use technical and organizational security measures to protect the data of which we become aware against accidental or intentional manipulation, loss, and destruction, and against access by unauthorized individuals. It is also a matter of course for us to guarantee that our data centers meet all the security standards under ISO/IEC 27001. We also impose our security standards on the service providers we use, whom we have obligated to comply with identical or comparable safeguards.

Our security measures are continuously revised in accordance with technological developments. To guarantee a high and up-to-date level of protection and security in digital data traffic (such as email and the use of our customer portal), we also use software to recognize malware that can be found in file attachments to emails, for example. Incoming digital messages are therefore checked for malware. This helps avoid unauthorized access to your and our data and contributes significantly to the protection from malicious programs, computer viruses, Trojans, spam messages, and the like.

Please note that electronic communication which uses standard email programs (such as MS Exchange) does not offer absolute protection from unauthorized access by third parties and that this form of communication transmission does not allow non-European servers to be enabled.

11 Your rights as a data subject

You have the rights to information (Art. 15 GDPR), rectification (Art. 16 GDPR), erasure (Art. 17 GDPR), restriction of processing (Art. 18 GDPR), and data portability (Art. 20 GDPR), and the right to object to the data processing (Art. 21 GDPR).

If you have given us your consent to the processing of personal data, you can withdraw that consent at any time. This also applies to declarations of consent that you gave us before the General Data Protection Regulation took effect. Please note that the withdrawal is only effective for the future. Processing that took place before the withdrawal is not affected.

General Privacy Policy

If you believe the processing of your personal data does not meet the requirements under data privacy law, please contact us to clear up your concerns.

You may also express your concerns about the processing of your data to a supervisory authority (Art. 77 GDPR); for example, to:

Austrian Data Protection Authority
Barichgasse 40-42
1030 Vienna
T +43 1 52 152 – 0
E dsb@dsb.gv.at

12 Miscellaneous

As part of ongoing technical advancements, we will update the information on data privacy if needed. You can find the current Policy on our website.