

Privacy Policy

ONLINE PRIVACY STATEMENT

Last Revised: This Privacy Policy shall be effective from 7 September 2026.

This is the privacy statement for BVNK Holdings Limited and all of its subsidiaries and affiliates (“**BVNK**”, “**we**”, “**us**”, “**our**”).

BVNK respects and protects the privacy of visitors to our websites, our customers who use our services and our customer’s end-users and transaction counterparties. To ensure transparency, this Privacy Policy describes our data handling practices when you (i) register, access or use content we own or operate on the websites located at www.bvnk.com, www.layer1.com, or any other associated websites we own or operate (each a “**BVNK Site**” and collectively the “**BVNK Sites**”); (ii) use our embedded services through an application programming interface(s) (“**API**”) on a third-party website; (iii) represent one of our clients; (iv) work with us as a service provider or introducer; (v) visit a BVNK office or register to attend a BVNK event; (vi) any other situation which requires the collection, use and disclosure of your personal data; or (vii) are an end user, counterparty, cardholder, wallet holder, payee, payer, or other individual whose personal data is processed by us because you are transacting with, receiving services from, or otherwise interacting with one of our customers who uses our infrastructure or embedded services.

Please take a moment to read through this Privacy Policy. If you have any specific questions about it, you’re welcome to contact us at dpo@bvnk.com, and we will be happy to give you further clarity.

Information about this Privacy Policy

This Privacy Policy outlines what data we collect from you, how we use this information, and the situations in which we disclose such information, in compliance with the relevant data protection laws, including but not limited to the General Data Protection Regulation (EU 2016/679) (“**GDPR**”), The Data Protection Act 2018 (“**DPA**”) and the GDPR, as incorporated under UK law within The UK Data Protection Act 2018 and amended from time to time (“**UK GDPR**”), the Spanish Data Protection Act (“**Organic Law 3/2018**”), the Data Protection Act (Chapter 586 of the Laws of Malta), the Singapore Personal Data Protection Act (“**SG PDPA**”) and the California Consumer Privacy Act (“**CCPA**”), as amended by the California Privacy Rights Act (“**CPRA**”) (each a “**Data Protection Law**” and collectively, the “**Data Protection Laws**”).

By accessing the BVNK Sites, using our service, and/or undertaking any other activity which may require the collection, use and disclosure of your personal data, you acknowledge that you have accessed and read this Privacy Policy, and you acknowledge that you have been informed of BVNK's collection, use and disclosure of your personal data.

Terms not otherwise defined in this Privacy Policy shall have the same meaning as is found in the applicable Data Protection Laws.

PRIVACY STATEMENT

Legal justification for processing personal data

Unless otherwise indicated, the processing of personal data refers to the collection, use and disclosure of personal data under the relevant Data Protection Laws. Where there is any inconsistency and/or conflict between the Data Protection Laws, the GDPR shall prevail.

Pursuant to Article 6 of the GDPR, BVNK shall only process your personal data if at least one of the following bases applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes ("**Consent**");
- processing is necessary, at the request of a data subject, to take steps before entering into a contract including performing verification of your identity and sending specific data to any relevant partners, as well as performing a contract, including contracts that you enter into with BVNK and sometimes with BVNK and a third party to support a specific product ("**Contract Performance**");
- processing is necessary for compliance with a legal obligation which we are subject to ("**Legal Obligations**"); and/or

processing is necessary for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child ("**Legitimate Interest**").

1. Consent

Where we process personal data as a result of consent, we ensure that consent is, where required, freely given, specific and informed, and established by a clear affirmative act. Where Consent is withdrawn, we have set out (below) how this may be undertaken by the data subject.

2. Contract Performance

Where we enter into a contract with third parties, processing of personal data may, as a matter of course, be necessary in order to execute such a contract or take pre-contract preparation steps.

3. Legal Obligations

Where there are legal obligations which apply to BVNK by virtue of any relevant Data Protection Laws, pursuant to other applicable laws or regulations (including regulatory obligations in the jurisdictions in which we operate), and/or an order of court or competent regulatory authority.

4. Legitimate Interest

Where BVNK has conducted and documented a legitimate interest assessment demonstrating that: (a) processing of personal data is necessary to pursue a legitimate interest of BVNK or a third party; (b) the processing is necessary for that purpose; and (c) the fundamental rights and freedoms of data subjects do not override those legitimate interests, BVNK may rely on the legitimate interests as the lawful basis (Article 6.1(f) of the GDPR) to process the personal data.

Where applicable, the individual will be provided with reasonable access to information concerning BVNK's processing of personal data on this basis.

Processing of Personal Data of End Users and Transaction Counterparties

In certain circumstances, BVNK may also collect the personal data of individuals who are not BVNK's direct customers. This occurs where BVNK provides infrastructure, embedded services, payment, wallet, card issuing, custody, or compliance services to its customers, and those customers use BVNK's services to interact with other individuals (for example, cardholders, wallet holders, transaction counterparties, payees, payers, merchants, or recipients of transfers).

Depending on the service and how BVNK's functionality is made available, these individuals may interact directly with BVNK's systems and accept our end-user terms, or we may process their personal data solely because they are transacting with or receiving funds from our customer without any direct interaction with us.

When you access BVNK services through one of our business customers or embedded partners, we share your personal data with that partner. Depending on the specific services and technical enablement (API or UI and related tooling), this may include your identity and contact details, onboarding and compliance verification status, account or wallet information, payment and transaction details, information about beneficiaries or transaction counterparties and your service usage data. We share this data to enable our partner to provide and administer the services to you, offer customer support, manage their relationship with you.

In such cases, we process this personal data based on:

- compliance with legal and regulatory obligations (including AML, CTF, sanctions screening, and travel rule requirements);
- the legitimate interests of our customers and/ or BVNK in enabling the secure and compliant provision of our customers services or our own services and product features; and/or
- the performance of our contractual obligations to our customers.

Where you share someone else's personal data with us (such as a payment recipient) you must have their permission to share their information with us or have another legal basis to provide their information. You are responsible for informing them that their data will be processed by BVNK, directing them to this Privacy Policy or explaining how we'll use their information and ensuring they understand their privacy rights.

When you send or receive assets, we're legally required to collect and share specific information about the transaction parties to comply with anti-money laundering and counter-terrorism financing regulations. We call this data 'travel rule data'. For more information on the data we collect, see "What categories and types of personal data does BVNK collect?" below. We share travel rule data with transaction counterparties and their service providers as required by law. Where you use BVNK services through one of our embedded partners, we may, where legally permitted to do so, share travel rule data about you or your transaction counterparties with that partner to enable them to administer and operate their services. Where such access is provided for the customer's or embedded partner's own administration, operation or management of its services, we rely on the legitimate interests of that customer or embedded partner, and/or BVNK, as applicable.

What categories and types of personal data does BVNK collect?

If you wish to use any of our services, we may collect and retain certain relevant data of yours, including some of your personal data.

We collect the following categories and types of personal data:

Category of Personal Data Collected	Type of Personal Data Collected
Identifiers	Names, Address, Date of Birth, Signature, Unique Identifiers/Personal Descriptors, IP Address, Cookies/Online Tracking Technologies, Communications from You, Email Address, KYC/KYB Documentation, Phone Number, Phone Country Code, Relationship Status, Account, Wallet and Payment Information, Transaction and Payment History, Sanctions, PEP and Adverse Media Screening Results, Fraud and Financial Crime Risk Indicators, and other data that may be necessary from time to time comply with applicable AML, CTF, sanctions and fraud prevention laws.
Sensitive Personal Data	Government Issued Identification Numbers, Nationality.
Financial Information	Transaction Information, Credit Information, Account Authentication Details, Contractual Details, Salary, Card Transaction History, Merchant Details, Spending Limits, BVNK Wallet Balance, Transaction Amount, Date/Time of Transaction.
Professional or Employment-Related Information	Socio-Demographic Details, Work Details, Employer, Profession and Education Background, Occupation.
Card & Service Operational Data	Card ID, Merchant Details, Fraud Check Data (for transaction screening), Dispute/Chargeback Data.
Internet or Other Technical Information	Details about your devices and technology that you use to access our services, Log Data (the type of browser you use, access times, pages viewed, and the page you visited before navigating to our Services), Device Information (data about the device you use to access our services, including information about the device's software and

	hardware, Media Access Control ("MAC") address and other unique device identifiers, device token, mobile network information and time zone).
Geolocation Data	Location.
Commercial Information	Products/Services Provided to You, Consumption Data (data about your consumption habits relating to your use of our services, including which purchases you make with both virtual and real currencies).
End User, Wallet and Counterparty Identifiers	Wallet address, wallet permissions/authorisations (permits), supported networks and currencies, wallet capability data (such as balances), persistent contact records relating to transaction counterparties, payers, payees, cardholders, and wallet holders.
Travel rule data	In respect of the transactions originator (sender) of a transfer of digital assets: • Full name of the individual transferring the digital assets. • The account number or Virtual Asset (VA) wallet address initiating the transfer. • Such of the following as are provided to BVNK in respect of the transfer: ○ Physical, residential or business address. ○ National identity number (e.g., passport number or government ID). ○ Customer identification number. ○ Date and place of birth. In respect of the transaction recipient (beneficiary) of a transfer of digital assets: • The legally registered name of the individual receiving the transfer. The account number or Virtual Asset (VA) wallet address receiving the transfer.
Tax and Automatic Exchange of Information Data	Tax residency information, jurisdiction(s) of tax residence, tax identification numbers, tax self-certification forms and documents, and any supporting information, and, where required by applicable tax reporting laws, information relating to an account, wallet, transactions, entity classification and controlling persons.

How does BVNK collect my personal data?

We collect your personal data directly from you. We may also collect personal data from third parties operating on our behalf, from third parties that connect to our embedded services via an API, from cookies and other online tracking technologies, from publicly

available resources, public records and information about you that is openly available on the internet; and from third-party service providers and partners where necessary to provide you with the services or products you have requested. We may also receive personal data from our customers where they submit information to us relating to their own end users, cardholders, wallet holders, or transaction counterparties in order to use BVNK’s services.

How does BVNK handle my personal data?

We will only process your personal data that is relevant for the purposes for which it is required to provide our services to you, which is further set out below. This may include providing infrastructure, embedded services, payment, wallet, card issuing, custody, or compliance services to our customers.

We may also process your personal data using artificial intelligence (AI). Artificial Intelligence (AI) is an umbrella term for a range of technologies that replace manual processes and solve complex tasks by carrying out functions that previously required human action. Tasks that we have traditionally done by thinking and reasoning are increasingly being done by, or with the help of, AI. For example, we use AI to enable us to more efficiently identify and review fraud and AML cases. Human input will always be required before a decision can be made in relation to any of these cases, in addition to any other measures BVNK deems necessary to ensure compliance with Data Protection Laws and the EU AI Act (as applicable).

Legal grounds we rely on to process your personal data

We will only process your personal data where we have a legally valid reason to do so. Under the GDPR, this is called a legal basis, and more than one legal basis may apply depending on the processing activity. The table below summarises the legal bases we rely on for each use of your personal data.

How we use your personal data	Personal data we may process	Legal grounds for Processing
To verify the identity of our customers	Full name, date of birth, nationality, government-issued identification (passport, ID, driver's license),	Performance of a contract: the processing of this personal data is necessary to provide our payment services to you, or is necessary as a pre-contractual step in order to provide these services.

	proof of address (utility bills/bank statements), and KYC/KYB documentation.	
For research and analytical purposes to provide, maintain, and improve the features, information security and functionality of our site and services	IP address, cookies and online tracking data, device information (operating system, browser type), log data (access times, pages viewed), and usage patterns.	Legitimate interest: we have a legitimate business need to use your personal data to enhance our service, training and information security.
For our own internal administrative and information management purposes, including managing our accounting records, analysis of financial results, internal audit requirements and receiving	Account records, transaction histories, billing details, customer service call audio transcripts, internal support tickets, audit trails, and communications between BVNK and corporate counterparties.	Legitimate interest: we have a legitimate business need to use your personal data to understand our business and monitor performance and maintain appropriate records; or Legal obligation: we may need to process your personal data to comply with certain legal obligations with regard to the security and operation of our systems and maintenance of accounting records; or Performance of a contract: properly managing your personal data to the extent necessary in order to provide our services to you.

professional advice		
Communicating updates about our services to you	Account administrator names, corporate email addresses, linked phone numbers, and communication channel preferences	Performance of a contract: we need to make sure you are aware of any material changes to our payment services in our order to perform our contractual obligations.
Communicating marketing information to you	Name, email address, phone number, marketing preferences, and interaction data with past campaigns, event attendance data, content downloads, tracking tokens from marketing emails (opens/clicks), and opt-in/opt-out status records.	Consent: where consent is required under applicable law, you or someone on your behalf has confirmed your consent; or Legitimate interest: where permitted by applicable law, we have a legitimate business need to tailor advertising to and market to customers and prospective customers who show an interest in us.
To perform real-time fraud and financial risk and where relevant, support our customers' or embedded partners' risk	Blockchain wallet addresses, transaction history, funds origin, risk scores, sanction lists/PEP screening results, IP addresses, and device telemetry and relevant Travel	Legal obligation: We have a legal and regulatory obligation to prevent, detect and investigate fraud and to identify and mitigate financial and AML/CTF risks; or Legitimate interest: we have a legitimate business need to carry out ongoing transaction monitoring to ensure our business remains compliant with our legal and regulatory obligations and where relevant, we and/or our customers or embedded partners have a legitimate

management activities	Rule data relating to transaction originators and beneficiaries.	interest in using relevant personal data to assess and manage fraud, financial crime and transaction risk.
To investigate, manage, and resolve disputes	Transaction records, customer support correspondence, account files, payment logs, and relevant communications from you.	Legitimate interest: we have a legitimate business need to recover any debt; or Establishment, defence or exercise of legal rights: such use is necessary for the purposes of establishing, exercising or defending our legal rights.
To process billing information and the collection of any fees owed to us	Bank account numbers, payment card/gateway info, invoice history, transaction values, and corporate billing names.	Performance of a contract: we need to process billing information and collect fees owed to us in order to deliver the payment services we contractually agreed to provide to you.
To comply with our legal obligations	Full KYC/AML file details, government-issued identifiers, tax information, audit logs, and regulatory correspondence.	Legal obligation: where applicable, we may process your personal data where we need to comply with a legal or regulatory obligation.
To protect and secure our business operations, systems and services	Login credentials, security event logs, firewall traffic, device identifiers, and network telemetry.	Legitimate interest: we have a legitimate business need to protect and secure our business operations, systems and services.

To use artificial intelligence (AI) tools and systems to support the provision of our services, including to assist with fraud detection and anti-money laundering checks, where appropriate and in accordance with applicable law.	Personal details of EPs (Merchants) and EPCs (End Customers), payment transaction records, device, login, session data and financial verification documentation (such as Source of Wealth or Source of Funds).	Legitimate interest: we have a legitimate business need to carry out ongoing transaction monitoring to ensure our business remains compliant with our legal and regulatory obligations. Legal obligation: We have a legal and regulatory obligation to prevent, detect and investigate fraud and to identify and mitigate financial and AML/CTF risks.
To comply with tax due diligence, reporting and automatic exchange of information obligations	Tax residency information, tax identification numbers, tax self-certification forms and documents and supporting information and, where required, identification information, account or wallet information, account balances or values, transaction information, entity classification and information relating to controlling persons.	Legal obligation: processing is necessary for us to comply with applicable tax due diligence, record-keeping and reporting obligations, including our obligations under CRS, CARF and other applicable automatic exchange of information requirements.

Will BVNK share my personal data with anyone else?

We do not sell your personal data. However, we may share your personal data in the manner and for the purposes described below:

- internally, including to our affiliated entities where necessary to provide you with our services or to manage our business;
- service providers assisting us in processing or otherwise fulfilling transactions and/or providing required services and/or products provided by third parties;
- with our customers and embedded partners through which BVNK services are made available to you. Depending on the relevant service, they may receive or have access to certain information about you and your use of the BVNK services where relevant to provide, administer, support or manage those services and their relationship with you;
- with third parties who help manage our business and deliver services, pursuant to a contract between the third party and BVNK, or pursuant to a contract between the third party and you. In these circumstances, the third party may be another controller, processor or sub-processor. Where the third party is a processor or a sub-processor, they are obliged, amongst other things, to keep your details secure, and to use them only to fulfil their contractual obligations to BVNK under a processing agreement or terms which comply with Data Protection Laws;
- with agencies including government and law enforcement agencies and organisations working to prevent fraud in financial services, including where requested as part of a routine inspection or investigation;
- with our regulators;
- to comply with all applicable laws, regulations and rules, and requests of law enforcement, regulatory and other governmental agencies;
- to comply with regulations commonly known as the “travel rule,” where we may collect counterparty information when you receive a deposit from outside of our service, or when you make a transfer to a wallet address outside of our service;
- as described above (see "**Processing of Personal Data of End Users and Transaction Counterparties**"), we may share travel rule data relating to end users and transaction counterparties with our embedded partners/ customers; and

- with the applicable local tax or revenue authority where we are required to do so under tax reporting and automatic exchange of information requirements, including CRS and CARF. For these reporting regimes, BVNK reports the required information to the applicable local tax authority, which may then exchange that information with tax authorities in other jurisdictions in accordance with applicable automatic exchange of information arrangements.

We also work with different types of third-party service providers, including:

- IT service providers;
- Third-Party Electronic ID Verification Service Vendors, including those that process biometric information;
- Vendors for tax reporting;
- Marketing and promotions providers (to promote our Services);
- Telecommunications technology providers (to send you messages, including SMS messages);
- CTF/AML service providers (for the purposes of transaction monitoring);
- Data hosting service providers and payment vendors (for off-site data hosting);
- Security service providers (for investigating fraud and security incidents);
- Analytics providers (to understand how you use our Services);
- Payment processing companies (to process transactions on our behalf);
- Document repository services providers;
- Customer support vendors; and
- Chatbots

Where we disclose your personal data to a third-party service provider, we will require that third party to protect your personal data and only use it for the purposes for which it has been disclosed, in accordance with applicable Data Protection Laws and our contractual requirements. These contractual requirements do not apply where we are required or permitted by law to disclose

personal data to a tax authority, regulator, government authority, law enforcement agency, court or other competent authority. Where a third-party service provider no longer requires your personal data to provide its services to us, it will be required to delete or otherwise handle that data in accordance with applicable retention requirements and its contractual obligations to BVNK.

We don't use your personal data to:

- send commercial or marketing messages to you, without your prior consent, unless we are permitted to do so under applicable law, or
- sell your data to third parties.

We operate globally

We provide our services on a global scale. As a result, the personal data we collect from you may be transferred to, stored and processed outside of the jurisdiction in which you live. The laws of those countries may vary from the laws applicable in your own country. For example, data gathered in the European Economic Area (“**EEA**”) [or United Kingdom \("UK"\)](#) may be transferred to, stored and processed at a destination(s) outside of the EEA [or UK \(as applicable\)](#). Said international data transfers will be carried out in strict compliance with the Data Protection Laws and, where applicable, after having executed the relevant safeguards for effecting any international data transfers, such as the International Data Transfer Agreement, the Standard Contractual Clauses, including the UK Addendum (as applicable) with the recipients of the data.

The collection of personal data and its processing prior to transfer are subject to the national laws where it is collected and/or where the data subject is located, and conditions for or restrictions on its transfer according to those laws are respected by BVNK.

Unless otherwise indicated, where your personal data is transferred out of the jurisdiction of which it is collected, BVNK will ensure that such personal data will continue to be protected by a standard of protection that is comparable to the protection the personal data would have had under the laws of the jurisdiction in which the personal data was collected.

Your account is stored by BVNK on a secure server maintained and operated by third-party service providers that may be located outside the EEA or UK from time to time. These third-party providers are bound by and adhere to the relevant data processing agreements, including in respect of international data transfers, at all times in compliance with Data Protection Laws.

How long do we keep records for?

We will only keep your personal data for as long as reasonably necessary to fulfil the relevant purposes set out in this policy and to comply with our legal and regulatory obligations. The period varies depending on the nature of the personal data and what we do with it, as well as our regulatory obligations.

Your data protection rights

Depending upon where you reside, certain choices and rights may be available to you under applicable Data Protection Laws. If you have questions about what rights may apply to you, please contact us at dpo@bvnk.com.

Subject to the applicable Data Protection Laws, you may have the right to:

- have access to your personal data by submitting a request to us;
- know the personal data we have collected about you, including:
 - the categories of personal data we have collected about you;
 - the categories of sources for the personal data we have collected about you;
 - the specific pieces of personal data we have collected about you;
 - our business or commercial purpose for collecting or selling your personal data; and
 - the categories of third parties to whom we have sold or shared your personal data, if any, and the categories of personal data that we have shared with each third-party recipient;
- have your personal data deleted;
- have your personal data corrected if it is inaccurate;
- have your personal data transferred to another third party of your choice;
- have the processing of your personal data restricted;
- object to further processing of your personal data, including to object to marketing from us or sharing for the purposes of cross-contextual behavioural advertising or profiling, to the extent applicable;

- make a data portability request;
- be notified as soon as practicable in the event that a material data breach occurs;
- withdraw any consent you have provided to us;
- restrict any automatic processing of your personal data to the extent applicable;
- limit our use of any sensitive personal data to those uses which are necessary to perform services or for other business purposes; and
- complain to the appropriate Supervisory Authority.

Residents of the State of California may also request a list of all third parties to which we have disclosed certain information during the preceding year for those third parties' direct marketing purposes.

For your protection, we will take steps to verify your identity before fulfilling any request. You also have the right to complain to a Supervisory Authority, in particular:

- a list of **European Union** data protection authorities can be found [here](#);
- the **United Kingdom's** data protection authority's contact details can be found [here](#);
- the **South African** data protection authority's contact details can be found [here](#);
- the **Singapore** data protection authority's contact details can be found [here](#); and
- the **California Privacy Protection Agency** contact details can be found [here](#).

Non-Discrimination: You will not receive any discriminatory treatment by us for the exercise of your privacy rights.

Do Not Track Requests

The BVNK Sites are not designed to respond to "do not track" requests from browsers.

Security measures for your personal data

We take all appropriate and reasonable technical and organisational measures to prevent the loss of, damage to or unauthorised destruction of personal data and the unlawful access to or processing of such data. We have systems in place to control your data in a way that minimises its exposure.

This includes adherence to the Payment Card Industry Data Security Standard (PCI DSS) for any processing or storage of cardholder data, where applicable, and is managed in partnership with our card issuing partner and processor.

We will take reasonable steps to identify all reasonably foreseeable internal and external risks posed to your personal data under our possession or control and establish and maintain appropriate safeguards against any risks identified.

Under what circumstances will BVNK contact me?

The personal data we process is subject to rigorous measures and procedures to minimise the risk of unauthorised access or disclosure. We will get in touch with you where this is required under Data Protection Laws.

Third-Party Links

We may provide links to other websites or resources provided by third parties. These links are provided for your convenience only. We have no control over the contents of those websites or resources and accept no responsibility for them or for any loss or damage that may arise from your use of them. If you decide to access any of the third-party links on the sites, you do so entirely at your own risk and subject to the terms and conditions of those websites.

Children

We do not knowingly collect personal data from children under the age of 13 through our BVNK Sites. If you are under 13, please do not give us any personal data. We encourage parents and legal guardians to monitor their children's internet usage and to help enforce this Privacy Notice by instructing their children never to provide us with personal data. If you have reason to believe that a child under the age of 13 has provided personal data to us, please contact us, and we will endeavour to delete that personal data from our databases.

Revisions to this Privacy Policy

This Privacy Policy may be revised from time to time so we can keep it up to date with global best practices and in accordance with the Data Protection Laws, you should check our website periodically to see our most up to date privacy notice, but we will always do our best let you know when we do via email.

CONTACT DETAILS

Email: dpo@bvnk.com

Address: 4th Floor, 91-93 Farringdon Road, London, EC1M 3LN, United Kingdom

Address: 160 Robinson Road, #14-04, Singapore 068914

Address: 365 Toni Stone Xing, Floor 3, San Francisco, CA 94158, USA

Address: C/ Sancho de Ávila 105, 08018, Barcelona, España

Address: Ruby Workspaces Office 3, Pendergardens, Triq Gort, San Gilijan STJ 9023, Malta

For US individuals, you may also call us at +1-888-315-0331