



Privacy Notice

Date : 10.09.2026

Document author:	DPO Office
Document owner:	DPO
Status:	FINAL
Date created:	20.08.2021
Version:	v6
Last updated:	August 2026
Security classification:	Public
Scope	Group

Modifications compared to the previous version of this Privacy Policy and entry into force

This updated privacy notice version 6.0 is applicable as from September 10, 2026.

You will find below the list of modifications compared to the previous version of our privacy notice :

- Section 4 : addition of the trust services and reorganisation /clarification of the purposes for which we may process the data.
- Section 7 : clarifications on the retention periods

Table of Contents

Introduction.....	4
1. Information about us.....	4
2. What is personal data?.....	5
3. What are my rights?.....	5
4. What personal data do we process & when?.....	6
4.1 Category of personal data and how they are collected.....	6
and legal grounds.....	7
5. Do we share your personal data?.....	11
6. International transfers of your personal data.....	12
7. How long will we keep your personal data?.....	12
8. How do we protect your personal data.....	13
9. Acting as a data processor.....	13
10. Changes to this Privacy Notice.....	13

Introduction

We understand that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of everyone who uses our services and/or uses our products and will only collect and use personal data in ways that are described here, and in a way that is consistent with our obligations and your rights under the General Data Protection Regulation (EU Regulation 2016/679) (the “GDPR”), or any other applicable data protection legislation.

This Privacy Notice applies where we are providing services to you and we are acting as a data controller (i.e. where we determine the purposes and means of the processing of that personal data) with respect to the personal data of

- Private users/consumers (natural persons using Banqup, BanqupID, qualified electronic signatures, qualified electronic seals or Payments services for their private use).
- Company users (natural persons using Banqup, BanqupID, qualified electronic signatures, qualified electronic seals, registered delivery or Payments services for their professional use) of specific services within Banqup/Billtobox; this may for instance be the case when you use our strong identification service or when you activate payment services (for example: when you pay your supplier invoices and access your bank statements). In order to unlock the payment services, you will need to go through an onboarding process, to register your company and verify your identity.
- Users and beneficiaries of payment services which are offered by Banqup SA (Payments) or its branch offices.

Please note that this Privacy Notice does not apply to other websites, applications or platforms offered by Banqup Group SA or its affiliates. We advise you to look at the relevant privacy notices when using such websites, applications or platforms.

Please read this Privacy Notice carefully and ensure that you understand it.

We also recommend that you read our relevant cookie policy when you use Banqup digital services such as Banqup websites or Banqup applications. It explains what cookies are, which ones are used by Banqup, how you can change your cookies preferences and how we protect your privacy. The cookie policy can always be found in the digital solution itself (link available at the bottom of the webpage).

1. Information about us

Banqup Group SA, with company number 0886.277.617 is a Belgium public listed company which operates in more than 15 countries via its affiliates as listed [here](#) (hereinafter referred to as “Banqup” or “we” or ‘us’). Banqup Group’s registered office is at Avenue Reine Astrid 92A, 1310 La Hulpe (Belgium).

In the event, you subscribe to our payments services or qualified trust services, these services are offered by Banqup SA, a limited liability company incorporated and existing under Belgian Law with registered address at Avenue Reine Astrid 92A, 1310 la Hulpe Belgium and with company number 0649.860.804, or where Banqup SA has a branch office or subsidiary.

You can contact our Data Protection Officer (‘DPO’) in writing at the following address: Banqup, for the attention of the DPO – Avenue Reine Astrid 92 A, 1310 La Hulpe, Belgium or by sending an email to gdpr@banqup.com.

2. What is personal data?

Personal data is defined as ‘any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier’. Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

The personal data that we use is set out in section 4 of this Privacy Notice.

3. What are my rights?

Under Data Protection legislation, you have the following rights, which we will always work to uphold:

- i. The right to be informed about our collection and use of your personal data. This Privacy Notice should tell you everything you need to know, but you can always contact us to find out more or to ask any questions.
- ii. The right to access the personal data we hold about you. If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a “data subject access request”.
- iii. The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete.
- iv. The right to be forgotten, i.e. the right to ask us to delete or otherwise dispose of any of your personal data that we have. Please note that this right is not absolute and can only be exercised if (i) we no longer need your personal data for the original purpose, (ii) if you withdraw your consent for processing it, (iii) if you object to us processing your personal data for our legitimate interest, (iv) if we unlawfully process your personal data or (v) if a local law requires us to erase your personal data.
- v. The right to restrict (i.e. prevent) the processing of your personal data. You have the right to ask us to restrict the use of your personal data if (i) you believe that the personal data which we hold is inaccurate, (ii) if we are processing the personal data unlawfully, (iii) you have objected to us processing your personal data for our legitimate interests or (iv) we no longer need the personal data for the purposes of processing but you want us to keep this for the establishment, exercise or defence of legal claims.
- vi. The right to object to us using your personal data for a particular purpose or purposes. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests (for example combating fraud), rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims
- vii. The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in a structured, commonly used and machine readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.
- viii. Rights relating to automated decision-making and profiling. You have the right not to be subject to decisions which may legally or significantly affect you and that were based solely on automated processing using your personal data. We will however not use your personal data in this way.

To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

For more information about our use of your personal data or exercising your rights as outlined above, we

advise you to consult our FAQs (if any) or we advise you to contact us via email (gdpr@banqup.com) or in writing to the following address: Banqup, Avenue Reine Astrid 92 A, 1310 La Hulpe, Belgium (for the attention of the DPO).

There is in principle no charge for exercising your right. If, however, your request is 'manifestly unfounded or excessive' (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your request within one month after receiving it. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. The contact details of your supervisory authority can be found [here](#). If you are located in Switzerland, please contact the [EDPIC](#). You may do so in the country of your habitual residence, your place of work or the place of the alleged infringement. We would welcome the opportunity to resolve your concerns ourselves, however, so please contact us first.

4. What personal data do we process & when?

In this section, we outline:

- The categories of personal data we collect and how they are collected (4.1)
- The purposes for which we process it. (4.2)
- The lawful bases we rely on under the GDPR. (4.3)

4.1 Category of personal data and how they are collected

Depending upon your use of our services (*i.e.* the services available in the Banqup/BilltoBox environment, payments related services, identification/trust services), we may collect some or all of the following personal data:

- **Identity data**, which allows us to identify you. These cover various kinds of data:
 - core identity data (including official identity documents): Depending on the identification means you choose, we may process your name, surname, address, phone number, email address, ID number, nationality, signature, fiscal code/social security number, electronic identification data. This personal data will be provided by you in the app or can be provided by the (local) identity provider to the extent that you would request the (local) identity provider to provide us with such personal data.
 - Unique identifier linked to your identity in your country of residence (such as, with regard to Belgium, the National register number). Such unique identifiers will only be used within the boundaries set by, and in accordance with, the applicable local laws and regulations.
 - Biometric data. As part of the identity verification process, if you opt for the biometric enrollment, we may process biometric data through a selfie video (liveness check). This biometric data will not be stored but is created and used for the duration of the comparison process with your official identification document.
 - If you act as a legal representative : Organisation name and organisation identifier (published in certificate); name, function/role and signature certificate of the authorised representative; supporting corporate documents (articles of association, trade register extract, mandate/power of attorney).
- **Account data** which includes your email address, phone number, account name, surname, specific capacity you are acting (employee or legal representative), company related info (if any) and job function. These are obtained from you when you enroll with our services.
- **Signature/Seal data** which are all such information, including personal data, as are necessary in

accordance with the applicable law in order to provide the trust service (qualified electronic signature and qualified electronic seal), under Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC) (the “eIDAS Regulation”). Signature data is a mixture of identity data and qualified certificate related data (status, serial numbers, IP address, authentication credentials).

- **Usage data & metadata** : which include IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. These are obtained directly from your device when you enroll or use our services.
- **Financial & transaction data** Financial Data includes : Bank account numbers, IBAN, SWIFT codes, and masked credit/debit card details (we adhere strictly to PCI-DSS standards). Transaction Data include: Amounts, timestamps, merchant details, currency, and payment status/history. If you have provided us with information in accordance with the provisions of the second Payment Services Directive (PSD II) as implemented in the relevant national laws, we may process withdrawals, amounts, notifications, payments to or from your Banqup Payment accounts or the payment account which you hold at other financial and/or payment institutions, data related to account statements, credit capacity, credit history and information about your payment accounts at other financial and/or payment institutions
- **KYC data**. Data which we process as part of our customer due diligence. This includes name, nationality, date of birth, national register number, country of birth, city of birth, country of residence, address, telephone number, e-mail address, ID card, politically exposed, shareholder percentage, card number, card type, date of issuance, place of issuance and the ID expiry date.
- **Document data** : When you are a consumer or sole trader, we may process data about you when you upload documents in our mobile application (like invoices or tickets). The documents data may include personal data (such as name, address, email, other personal data included in the invoice) about you or related to third parties. This data is always provided by you.

4.2. Purposes of the processing and legal grounds

We only process the above personal data as are necessary for the purposes described below and we only process data that is, in relation to said functions or services, adequate, relevant and limited to what is necessary.

We only process your personal data on the basis of one of the following legal grounds:

- processing that is necessary for the performance of the contract between you and Banqup (including the preparation, execution and termination of the contract);
- processing for which you have given (explicit) consent – it being understood that Banqup will at all times ensure that that consent is compliant with the applicable laws and regulations: e.g. processing biometric data to verify your identity when you register for a Banqup account.
- processing that is necessary for the purposes of the legitimate interests pursued by Banqup : e.g. maintaining platform security and integrity, preventing fraud. Where we rely on legitimate interest (Article 6(1)(f) GDPR) as a lawful basis for processing, we have conducted a Legitimate Interest Assessment (LIA) to balance our commercial and operational needs against your privacy rights and expectations.
- processing that is necessary for compliance with a legal obligation to which Banqup is subject: e.g. (i) anti- money laundering and terrorist financing laws and regulations, (ii) compliance with legislation relating to sanctions and embargoes, (iii) tax legislation (e.g. to prevent tax fraud or to comply with our notification obligations, (iv) applicable financial regulations (v) eIDAS Regulation. In addition we may process personal data in order to reply to an official request from a duly authorised public or judicial authority.

Purposes of the processing	Category of data	Lawful basis
----------------------------	------------------	--------------

Registration on our platform and logging in	Account data Identity data	Performance of the contract Legitimate interest (maintaining platform security and integrity and preventing fraud, securely authenticate users for logging into the entire Banqup ecosystem ensuring seamless single sign-on).
Billing, Subscription, Account Management and other administrative purposes - Managing customer accounts, subscription, platform access, and collecting software fees.	Account data	Performance of the contract if you are a consumer or a sole trader. In all other cases, our legal basis will be our legitimate interest (managing commercial relationships, executing client contracts with corporate entities, and collecting fees for B2B accounts).
Identity Verification for Certificate Issuance (trust services) - Verifying your identity to issue qualified electronic signatures, seals, and timestamp certificates. We also verify the legal capacity when you represent and act on behalf of a company.	Identity data Biometric data (if video/liveness check is used by comparing the picture from the official document with the selfie video)	Legal obligation Explicit consent
Signature/Seal creation - generating qualified electronic signature or seal	Signature data Account data	Legal obligation Performance of the contract
E-payments services - Processing payment transactions, initiating transfers, and enforcing Strong Customer Authentication (SCA).	Financial & Transaction data	Performance of a contract Legal obligation
AML & Counter-Terrorist Financing Compliance - Screening users, conducting customer due diligence, and monitoring payment transactions against sanctions lists.	KYC data, Financial & Transaction data Identity data	Legal obligation Legitimate interest
Fraud monitoring and prevention - monitoring fraud, cyber and credit risk.	Financial & Transaction data Identity data	Legitimate interest (ensuring network and information security, preventing cyber incidents, and protecting payment infrastructure).
Customer due diligence (KYC) - to prevent fraudulent conduct or behaviour that contravenes international sanctions and to comply with regulations against money laundering, terrorism financing and tax fraud.	KYC Data	Legitimate interest Legal obligation
Customer support (helpdesk) & troubleshooting - Responding to	Account data and any other personal data available in	Performance of the contract if you are a consumer or a sole trader.

technical inquiries, troubleshooting user issues, and managing platform tickets.	support communication, ticket history, logs, user screenshots.	In all other cases, our legal basis will be our legitimate interest (ensuring operational service continuity and delivering technical support to corporate end-users).
Direct Marketing & Service Updates - Sending product updates and promotional offers regarding similar trust, payment, or invoicing features.	Account data	Legitimate interest (soft opt-in for existing users for marketing similar products) or Consent (where required by local e-privacy laws).
Product Improvement & Platform Analytics - Analyzing platform usability and tracking traffic to optimize user experience and feature design.	Usage data and Metadata	Legitimate interest, namely monitoring and improving our application to ensure the best possible customer experience. However, where we collect usage data through non-essential cookies, we may request your consent.
Defense of Legal Claims & Dispute Resolution - Resolving non-repudiation claims on electronic signatures, handling payment chargebacks, or managing litigation (establish, exercise, or defense of legal claims (administrative, out-of-court, or judicial proceedings).	All category of data, that are necessary for the establishment, exercise or defence of legal claims	Legitimate Interest (protecting the company's legal position and resolving disputes).
Platform Security, Fraud Prevention & Continuity - Protecting systems against cyber threats, preventing payment fraud, and ensuring service availability.	Usage data and Metadata Account data Identity data Financial & Transaction data	Legitimate Interest (ensuring a secure SaaS environment)
E-Invoicing & statutory tax record keeping - Generating, transmitting, and archiving electronic invoices.	Documents data	Performance of the contract
Audit Logging & Archiving - maintaining legally required trust service logs signature and verification trails.	Usage data and metadata Signature data	Legal obligation
Handling Data Subjects Rights Request (according to GDPR)	Identity data and any other data necessary to handle the request appropriately	Legitimate interest (ensuring compliance with data protection laws and responding to Data subject requests)

In certain cases, we may process **sensitive personal data**. Sensitive personal data is data relating to your

health, ethnicity, religious or political beliefs, genetic or biometric data or criminal data (e.g. information on fraud). We will only process such data if:

- we have your explicit consent, or
- we are required to do so by the applicable local law (e.g. in connection with money laundering or terrorism financing monitoring)

The above data may be obtained in any of the following ways:

- i. if shared by you with us when you become a customer, register for our services or make use of our services;
- ii. from your organisation when it becomes a customer
- iii. from available third-party services (e.g. publications/data bases made available by official authorities or our corporate clients and/or services providers.)

We will not sell your personal data to third parties and will only use your personal data for the purpose(s) for which it was originally collected unless we reasonably believe that another purpose is compatible with that or those original purpose(s) and need to use your personal data for that purpose. If we do use your personal data in this way and you wish us to explain how the new purpose is compatible with the original, please contact us. If we need to use your personal data for a purpose that is unrelated to, or incompatible with, the purpose(s) for which it was originally collected, we will inform you and explain the legal basis which allows us to do so. In some circumstances, where permitted or required by law, we may process your personal data without your knowledge or consent. This will only be done within the bounds of the GDPR or other applicable data protection laws and your legal rights.

5. Do we share your personal data?

Use of sub-processor(s)

We are free to rely on data processors (which may include any member of the Banqupgroup). A processor is the natural or legal person who processes your personal data upon request and on behalf of us, the controller. The processor is required to ensure the security and confidentiality of the personal data. The processor will always act on our instructions. We rely on processors for application, security or infrastructure purposes, administrative purposes, customer onboarding, identification and prevention of fraud, analytic purposes and communication purposes.

With a view to the optimal protection of your personal data, we have made the necessary contractual arrangements with our processors to ensure that they apply the highest privacy standards. In any event, data processors shall be required to have the necessary technical and organisational measures in place to protect the personal data.

Sharing of personal data with third parties (other than sub-processors)

In some circumstances we may share certain of your data. Such sharing can be internally, *i.e.* with other affiliates of the Banqupgroup or externally, *i.e.* with other third parties.

<u>Internal/external</u>	<u>Details on sharing</u>
Internally	We may share certain data with other affiliates of the BanqupGroup in order to provide you with certain services offered by our affiliates. We will only do so if we have a legitimate basis to share such data and shall request your consent where such would be required.
Externally	We may share certain data with or receive certain data from: - Third parties designated by you. This can be beneficiaries of your payments or third parties to whom you consented (e.g. eID identity providers). Within the framework of the second Payments Services Directive (PSD2) we may

	be obliged to share data with so-called third-party providers (TPP's) to retrieve account information and/or initiate payments. Similarly we might receive personal data ourselves if we would be providing services as TPP and you explicitly consent to receiving such services; - Public and/or tax authorities, regulators and supervisory bodies in order to comply with our legal and regulatory obligations; - Judicial and/or investigative authorities (e.g. the police, public prosecutors or courts); - Sources within the public domain such as the national company register or central account register; - Financial institutions, payment clearing and settlement institutions (i.e. SWIFT) and card scheme providers (e.g. Visa and Mastercard) in order to process and facilitate payment transactions; - Postal services, if such would be required to contact you; - The <i>ombudsman</i> (or similar extrajudicial mediation services) to whom you file a complaint.
--	--

6. International transfers of your personal data

In certain circumstances, we may store or transfer some or all of your personal data in countries that are not part of the EEA. This might for instance be the case when we are making use of processors who make use of specific sub-processors. These are known as "third countries" and may not have data protection laws that are as strong as those in the EEA. This means that we will take additional steps in order to ensure that your personal data is treated just as safely and securely as it would be within the EEA and under the Data Protection Legislation as follows:

We transfer your personal data to third countries whose levels of data protection are deemed 'adequate' by the European Commission or the Swiss Federal Council. More information is available from the [European Commission](#), [ICO](#) and the [FDPIC](#) websites.

We use specific contracts with external third parties that are approved by the European Commission for the transfer of personal data to third countries. These contracts require the same levels of personal data protection that would apply under the GDPR or the Swiss FADP.

If you are located outside the EEA, similar restrictions apply.

Please contact us for further information about the particular data protection mechanisms used by us when transferring your personal data to a third country.

7. How long will we keep your personal data?

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was originally collected. After that we will, in accordance with the applicable laws and regulations, delete your personal data, anonymize it or aggregate the data to a level that it can no longer be identified.

The effective retention period depends on the specific legal, regulatory or operational requirements applicable to each category of data :

- Commercial Contracts & Account Administration: Personal data linked to your account, subscription, and contractual relationship with Banqup is retained for the duration of the contract and for 10 years following the termination of the contract.
- Accounting & Tax Records (E-Invoicing, Billing, Payment History): Financial transactions, invoices,

and accounting documentation are retained for 10 years following the end of the financial year to which they correspond.

- Anti-Money Laundering (AML) & KYC Compliance: Personal data processed for customer due diligence, sanctions screening, and AML/CTF compliance is retained for 10 years following the end of the business relationship or execution of an occasional transaction, in accordance with applicable anti-money laundering legislation.
- Qualified Trust Services (eIDAS): Data relating to issued qualified certificates, timestamping, and evidence of electronic registered deliveries is retained for a minimum of 7 years following issuance, in accordance with Regulation (EU) No 910/2014 (eIDAS) and national trust service legislation.
- Biometric Data: Biometric data collected during real-time identity verification (liveness check) is strictly used for immediate comparison against official identification documents and is discarded immediately once the verification process is complete.
- Platform Analytics: Usage data & metadata are retained for 90 days from collection, unless linked to trust services or an ongoing dispute or legal claim.

8. How do we protect your personal data

The security of your personal data is essential to us, and to protect your data we will take appropriate technical and organisational precautions. This means that we have the necessary policies and procedures and IT security measures in place to ensure the confidentiality and integrity of your personal data. These policies, procedures and measures are periodically updated to keep them in line with regulations and market developments.

Internal access to the personal data is limited on a strict 'need-to-know' basis. Only authorised personnel, whose activity will be monitored to prevent any misuse, will be able to access the personal data.

9. Acting as a data processor

In respect of other data collected through Banqup/Billtobox, Collect and Channel, we do not act as a data controller; instead, we act as a data processor. Insofar as we act as a data processor rather than a data controller, this notice shall not apply. Our legal rights and obligations as a data processor are instead set out in the contract between us and the relevant data controller. These can be found in the applicable terms and conditions.

10. Changes to this Privacy Notice

We reserve the right to change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our platform/application in a way that affects personal data processing. We always indicate the date the changes were published and you can still access our archived versions for your review. If you wish to access the privacy notices archive please contact our DPO via gdpr@banqup.com.

Every change will be published on our platform or through our other usual communication channels.

This privacy notice is effective from September 10, 2026.