Banqup Group Global Privacy Notice

Last update : December 12th, 2025

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"), the Data Protection Act of 2018 (hereinafter: UK GDPR) or any other 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, or Payments services for their private use).
- Company users (natural persons using Banqup, BanqupID, or Payments services for their proffessional 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 BanqupPayments SA or its branch offices.

Please note that this Privacy Notice does not apply to other websites, applications or platforms offered by BanqupGroup 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 Banqupdigital services such as Banqupwebsites or Banqupapplications. It explains what cookies are, which ones are used by Unifiedpost, 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

BanqupGroup SA, with company number 0886.277.617 is a Belgium public listed company which operates in more than 20 countries via its affiliates as listed here (hereinafter referred to as "Unifiedpost" or "we" or 'us'). BanqupGroup's registered office is at Avenue Reine Astrid 92 A, 1310 La Hulpe (Belgium).

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

You can contact our Data Protection Officer ('DPO') in writing at the following address: Unifiedpost, for the attention of the DPO – Avenue Reine Astrid 92 A, 1310 La Hulpe, Belgium or by sending an email to

gdpr@unifiedpost.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:

- 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.
- 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 "subject access request".
- The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete.
- 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.
- 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.
- 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
- 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.
- 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@unifiedpost.com) or in writing to the following address: Unifiedpost, 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 the UK, please contact the ICO. If you are located in Switzerland, please contact the FDPIC. 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?

In this section we have set out:

a) the general categories of personal data that we may process;

b) the purposes for which we may process personal data; and

c) the legal bases of the processing.

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

Category	**Description, purposes & legal basis**
Account data	We may process your account data ("**Account data**"). The Account data includes your email address, phone number and account name. The Account data may be processed for the purposes of providing our services (register or identify yourself, login into the application,communicate with you and send service notifications). The legal basis for this processing is the performance of a contract between you and us. We can also send marketing communication based on our legitimate interest. However you have the possibility to opt out from such communication via the unsubscribe link available in each marketing communication.
Billing data	We may process your data for billing (invoicing), account management and other administrative purposes. Billing data may include your email, phone number, name,

	surname, address, company related information (if any). We may send you an email containing your invoice, if applicable. The legal basis for this processing is the performance of a contract between you and us if you are a consumer or a sole trader. In all other cases, our legal basis will be our legitimate interest.
Documents 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. The documents data shall be processed for the purpose of providing you the services. The legal basis for this processing is the performance of the contract between you and us.
Usage Data/Metadata	We may process data about your use of our application ("usage data"). The usage data may include your 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. The source of the usage data is our analytics tracking system. This usage data may be processed for the purposes of analysing the use of our services and sending you specific services notifications. The legal basis for this processing is our legitimate interests, 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.
Identification Data	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 (“Identification data”) ● to comply with our legal obligations and statutory requirements, including (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. In addition we may process personal data in order to reply to an official request from a duly authorised public or judicial authority., ● to prove your identity (strong customer authentication) within the entire Banqupecosystem in order to avoid repeatedly asking for identification related personal data. The legal basis for processing is your consent. Note that if you do not give your consent, you will not be able to use our identification process for the purpose of login into our platforms. 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. Please note that we will only process your ID number to the extent that such is permitted by the applicable law.
Financial and transaction Data	If you have provide 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 BanqupPayment 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 ("Financial & Transaction data"). We may process Financial and Transaction data ● to comply with our legal obligations and statutory requirements, including (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 . In addition we may process personal data in order to reply to an official request from a duly authorised public or judicial authority. ● on the basis of legitimate interest for the following purposes: (i) for detection and prevention of fraud, cyber and credit risks, (ii) for internal reporting and/or internal control (*i.e.* to assess potential risks within Unifiedpost), (iii) for maintaining insurance coverage, (iv) for marketing purposes (*i.e.* to offer similar products or services), (v) necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure, (vi) for sharing data with third parties if you subscribe to our factoring services. ● upon receipt of your consent. This will be the case when (i) you grant us the right to use PSD2 data when we are acting as third party provider, (ii) we are processing biometric data for identification purposes or (iii) to answer questions of third parties (unless we have another legal basis such as compliance with our legal obligations).
KYC Data	Data which we process as part of our customer due diligence and to prevent fraudulent conduct or behaviour that contravenes international sanctions and to comply with regulations against money laundering, terrorism financing and tax fraud. 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.
Data obtained via others	Data which we have obtained from other Banqupaffiliates or other third parties, such as the relevant national register, the official national gazettes or data from external companies which Banquppayments processes based on its legitimate interest.
Biometric data	As part of the identity verification process, we may process biometric data through a selfie or video for the purpose of comparing the picture taken from the official identification document presented by you or the (local) identity provider with the liveness check. This biometric data will not be stored but is created and used for the duration of this comparison process. The legal basis for this processing is your explicit consent.

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:

- if shared by you with us when you become a customer, register for our services or make use of our services;
- from your organisation when it becomes a customer
- 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, the UK 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.

Internal/external	Details on sharing
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 *ombudsman* (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, the UK government 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, UK GDPR, 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 may depend on the circumstances. Often such a retention period is defined by a specific law. For instance: personal data which is obtained within the framework of anti-money laundering must be kept for a period of 10 years after the end of the contractual relationship or the transaction has been executed. Where there is no specific legal requirement, we will look at the applicable

statutes of limitations and keep your personal data for such a period. In most cases this will be 10 years after the end of the contractual relationship that we have with you, but it is possible that we use a shorter retention period. For example: your biometric data is only used during the processing to establish your identity, then discarded.

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.

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

This privacy notice is effective from December 12, 2025.