Privacy Statement

1. General information

This Privacy Statement applies to the "Bancontact Pay" application (the "App"), and describes how and to what extent we collect and use your personal information (personal data) when you install, activate and use our App.

The App is a mobile e-payment application owned and operated by Bancontact Company SA/NV (hereinafter referred to as "we", "us", "our"), with registered headquarters located rue d'Arlon 82, 1040 Brussels, Belgium.

Upon your acceptance of the applicable Terms and Conditions, the App enables you to register up to five (5) Bancontact Cards from multiple card issuers, allowing you to make "peer to peer" (P2P) and "peer to merchant" (P2M) Mobile Bancontact Transactions in euros with your mobile device such as a smartphone or tablet.

This Privacy Statement will be updated from time to time to reflect regulatory changes and/or technological and service developments and implementation into the App. Any updates to this Privacy Statement will be notified to you in due time, via notifications in our App and/or via service e-mails.

Note that our App may provide links to third-party websites or allow you to access third-party services. Please beware that we have no control over the way these third-party websites or third-party service providers collect and process your personal data when you make use of them. When visiting those links, make sure you review first their privacy statements before providing any personal data to them.

2. Who is responsible for processing your personal data

For the purpose of the applicable data protection laws, Bancontact Company SA, is the data controller.

Bancontact Company SA/NV
Rue d'Arlon 82, 1040-Brussels, Belgium
www.bancontact.com
DPO : dpo@bancontact.com

For Bancontact card issuers, please refer to the card issuer's privacy statement. For the other providers, please refer to the menu *Services* for each service. The list may evolve from time to time, as we aim at rendering our App even more attractive by proposing you access to additional third-party services through our App.

Note that in order to make use of the services provided by a third-party services provider you will have to review and accept its respective terms and conditions and its privacy statement. As for your loyalty cards you may register and use in the App, these remain subject to the terms and conditions and privacy statement of the respective issuer of such loyalty card.

For additional information on how we process your personal data, or for exercising your rights under the applicable data protection laws, you may contact our Data Protection Officer ("DPO") via email or via regular postal services.

3. Personal data we process

When installing, activating and using our App, we may collect, process and store certain of your personal data, as follows:

3.1. data related to your mobile device, such as:

- the manufacturer, the model name and model number;
- the version of the operating system (OS);
- your choice of language, as recorded in your mobile device OS: NL/FR/EN;
- the IP address;

3.2. data you provide to us when activating or using the App, such as:

- your acceptance of our Terms and Conditions, with time of acceptance;
- your name and surname;;
- your mobile phone number;
- your e-mail address;
- your choice to receive communications by email, or not;
- the number (in a truncated form) of your card(s) which you chose to register with the App;
- a derived value of the PIN (unreadable format) chosen during the activation and registration process with our App, authorising e-payment transactions;
- Bancontact transaction details, for instance the amount of the transaction and the date and time the transaction was made; details regarding the approval of payments; message details if you chose to add a message to your payment;
- a derived value of your log-in tokens (unreadable format) to use third party services you access through the App via the menu *Services*;For identification and identity verification purposes (as required by the Belgian anti-money laundering law of 18 September 2017) we may also obtain some of the above information on you (including your name and surname);
- if you use the bill payment feature proposed in the App and with your consent, your national register number, with masked characters, as an extra method to identify and authenticate you, more precisely to ensure that you are correctly matched to (the payment of) an invoice and (only) get access to your own invoice(s). Please note that for this specific use case, you would provide us with that information through Itsme, in a secured and encrypted format, without the possibility for us to read this information in full. The unique purpose of this processing is to ensure we can properly identify and authenticate you when using our application, in order to ensure the linked invoices are the ones you should receive. This data will not be used for other purposes, nor be stored by us. Neither will it be used as a unique identifier. You can revoke your consent or restrict the processing at any given moment by contacting our Data Protection Officer at dpo@bancontact.com. The partner providing us with this invoice feature is POM, which has a publicly available privacy notice on https://www.pom.be/en/privacy.

3.3. data pertaining to the App or to your account, such as:

- the App ID or token (i.e.: unique identifier for the App you installed);
- time and date when our App was installed on your mobile device;

- the App status (active or not);
- your Bancontact account ID, and its status (active, suspended or revoked);
- time of the last contact between the App and Bancontact related systems;
- usage of the App, for instance which screens you open and how much time you spend in the App.

3.4. data provided when you contact us, such as:

- the name(s), (e-mail) addresses and phone number(s) mentioned in your messages to us;
- the content of any message sent to us;
- any other information you chose to provide to us upon our request, such as proof of your identity.

3.5. data (card number) related to the loyalty cards you have received from your retailer, when you register them in the App.

3.6. in order to enable certain App features and subject to your express consent we may have access to the contacts on your phone address book.

For the avoidance of doubt, Bancontact Company does not collect nor process any of your special categories of personal data when you choose to enable the use of your mobile device Biometric ID (such as your fingerprint or face scan), to identify yourself or to authenticate your payments in the App. If you choose to use an alternative solution to the Mobile PIN (such as the use of Biometric ID) to identify yourself and authorize Mobile Bancontact Transactions in the App, the responsibility for collecting and processing any of your biometric data falls upon the provider of such an alternative authentication solution and/or upon the provider of the mobile device operating system.

The processed data might be shared with banks, partners, merchants, or in some situations other App users, to correctly process your payments, their reconciliations, refunds and post-settlement support, but also to prevent and detect fraudulent activities. This is done in order to ensure proper functioning of the provided services, according to our Terms and Conditions and contractual agreements in place.

4. Why and how do we use your personal data

We use your personal data for specific purposes and only when it is necessary to perform (or enter into) our contract with you, and/or to fulfil our legal obligations, and/or for our legitimate interests (to the extent that such legitimate interests are not overridden by your interests), or when we have obtained your prior consent. We collect and process your personal data:

- to register you as a new user of our App, or to identify you as an existing registered user;
- to carry out our obligations arising from your acceptance of the Terms and Conditions for the use of our App;
- to support us in the qualitative delivery of the technical and payment services toward our customers, according to the contractual obligations;
- to comply with our own regulatory obligations as a payment institution under the supervision of the National Bank of Belgium, when the App is used to pay a merchant, such as: fight against money laundering and terrorism financing, but also sanctions screening;
- to ensure that you, as a registered App user, observe and carry out your obligations for the use of the App, arisen from your acceptance of our Terms and Conditions;
- to provide you safe access to the information and services provided by our App;

- to ensure the safety and confirmation of your e-payment transactions and to verify their legal compliance;
- to facilitate payments between you and other App users. For this process, our App will request access to the contacts on your phone address book and we process the first name and last name of those who make payments to you or to whom you make payments. We will also process the message details you include with your payment;
- to provide you the possibility to review your transaction history;
- to provide you with adequate support when you request if from us;
- to enable you to regain access to your account (payment methods, loyalty cards, third party services, transaction history) when you reinstall the App or switch to another mobile device;
- to notify you (with in-app messages or service e-mails) about changes to our App or any other aspects connected to our App and services, including, but not limited to, changes to our App Privacy Statement;
- to offer you in-app rewards, discounts and promotional deals that are available only via our App;
- to monitor App crash events via Google Firebase;
- to monitor specific App triggering events (like adding a Bancontact card,) via Mixpanel and Insider for technical and operational purposes or to provide you with in-app messages;
- to improve our App and ensure that its content is the most relevant for you and adapted to your mobile device and to improve the service;
  We store and analyse your (transaction) data for purposes of improving our services. Such data is used for example to improve the user-friendliness of the App. For this purpose, we analyse users' click behaviour in the App on an aggregate level, the time spent on the App and usage of specific features of the App;
- to perform statistical analysis of your transaction data;
- based upon your consent (opt-in), to provide you, from time to time, with information on similar products and services we offer. For example, we use your name to address you personally in e-mails and/or in-app messages and we use your language settings to write to you in the language of your preference (when supported).
  If you do not want us to use your personal data for direct marketing purposes, or wish to withdraw your consent for direct marketing, you may do so by using the "unsubscribe" link provided in each such communication, or by sliding "off" the switch "Newsletters" in the menu "Settings" of our App;
- for fraud prevention purposes, we store your transaction data and device information, including information about the merchants from whom you purchased products or services, your personal data and information concerning your approval for the execution of payments. We also process your IP address, device manufacturer and device model in that context. We do this in order to prevent fraudulent use and limit our exposure to any risks, as well as preventing, investigating and countering (attempted) unlawful and undesirable activities targeted at you, us, our customers and staff or any other party, and for participating in internal and external warning systems.

Subject to your express consent we may need to have access to the following services on your smartphone or tablet:

- your camera, to scan QR codes;
- notifications.

You can revoke your consent for the above in the settings of your mobile device.

We take appropriate security measures to prevent misuse and unauthorised access to your personal data. In doing so, we make sure that only the necessary persons will have access to your personal data, and that access to your personal data is protected in accordance with applicable data protection laws.

In the delivery of our services we make use of third parties such as professional advisors (f.i. auditors and lawyers), partners (banks and payment service providers) and subcontractors (such as data hosting providers and other technology service providers). These third parties are subject to binding contractual obligations to only use your personal data in accordance with our prior written instructions and to use measures to protect the confidentiality and security of the personal data. Some of these third parties are located outside the European Economic Area (EEA), but we only share your personal data with third parties in countries that provide an adequate level of protection or when appropriate safeguards are in place.

We call upon Telesign to assist us in trying to detect fraudulent phone numbers during the onboarding process in the App. Your personal data will therefore be processed by Telesign, which also reuses them to provide fraud prevention services to its customers. Telesign thereby helps us and its other customers keep the Internet safe and protect websites against fraud. For more information about the processing of your data for which Telesign is responsible as controller and your rights in that respect, see Telesign's privacy notice https://www.telesign.com/privacy-notice.

We use artificial intelligence (AI) technology such as generative AI, to support our internal operations, specifically to assist our staff in drafting responses to frequently asked questions. These tools are securely designed to enhance efficiency and ensure consistent and timely treatment of the received questions. . The AI does not have access to our customers profiles and data bases, and the environment in which it is used is segregated from other internal or external systems. The highest technical and organisational security measures have been implemented.

The data processed by the AI system is limited to the content of recurring inquiries and does not involve profiling, automated decision-making, or behavioural analysis. All AI usage is aligned with applicable data protection laws, including the General Data Protection Regulation (GDPR), and we ensure that any AI system used meets the ethics, transparency and accountability requirements of the European AI Regulation.

If you have concerns about how your data is processed, you can contact our Data Protection Officer at dpo@bancontact.com

5. How long do we keep your data

The period for which we retain information about you varies depending on the type of information and the purposes we use it for. In general, we retain your (personal) data for 18 months to allow you easier reinstallation and use of our services after a short period of inactivity. After 18 months of inactivity, or on the date you delete your account, your data will be erased. Please note that regarding your transactional information when paying a merchant through the app, according to the article 60 of the Belgian Anti Money Laundering Law, we are obliged to retain this data for a period of 10 years based on the date on which the transaction occurred.

6. Exercising your rights

When using our App, you are guaranteed the exercise of a number of individual rights as provided under the GDPR and the Belgian Data Protection Act of 30 July 2018, such as the right to:

- contact us requesting information on what data we have on you;
- rectify any erroneous personal data you (may) have submitted;
- export your personal data to a third party of your choosing;
- object or restrict, under specific circumstances, the processing of your personal data;
- request the removal of your personal data, where such removal is permitted under the applicable laws.

Should you wish to exercise any of these rights, you may do so by submitting an e-mail request to our Data Protection Officer (dpo@bancontact.com). When you contact us, please be specific as to what information you require, or what right you wish to exercise. In order to prevent any abuse or identity fraud, we may ask you to provide additional information and/or to provide an adequate proof of your identity (such as a copy of your ID card or passport). A response to your request shall be provided within the timeframe established by the applicable law.

If you believe that your rights with regard to the protection of your personal data are not uphold, you may submit a complaint to our DPO or, alternatively, you may choose to file your complaint with the Belgian Data Protection Supervisory Authority, via email at: contact@apd-gba.be or via post at: rue de la Presse 35, 1000 Brussels, Belgium.

Last update: 05/05/2026