

Privacy Statement

Version: 2026-01/ Applicable as of: 01.03.2026.

- [1. General information](#)
- [2. Who is responsible for collecting and processing of your personal data?](#)
- [3. Personal data we may collect and process](#)
- [4. Use of cookies, web beacons and similar technologies](#)
- [5. Why do we process this data and for how long?](#)
- [6. Are we allowed to process your personal data?](#)
- [7. Do we share or transfer your personal data?](#)
- [8. Exercising your rights](#)

1. General Information

1.1 The www.bancontact.com website (hereinafter: “**Websites**”) is owned and operated by **Bancontact Company NV/SA**.

Bancontact Company NV/SA (hereinafter referred to as “**we**”, “**us**”, “**our**”) is a Belgian registered company, under No. 0675 984 882 RPR/RPM Brussels, with its registered headquarters located at: Rue d’Arlon 82, 1040-Brussels, Belgium.

1.2 This Privacy Statement applies specifically to **Websites** and describes if, how and to what extent we collect and process your personal data when you access, navigate and use our websites.

1.3 This Privacy Statement will be updated from time to time to reflect regulatory changes and/or technological developments and implementation into our websites. Any updates to this Privacy Statement will be notified to you in due time through posting the updated version on our websites or through other available channels. Our websites Privacy Statement applies as of the date stated above and replaces prior versions as of this date.

2. Who is responsible for collecting and processing of your personal data?

2.1 For the purpose of the applicable data protection laws, we are the responsible entity (the ‘*data controller*’) for the processing of the personal data you provide to us when you visit and make use of our Websites.

2.2 For additional information on how we collect and process your personal data, or for exercising your rights under the applicable data protection laws, you may contact our Data Protection Officer (‘DPO’) at the address mentioned below.

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

2.3 Our websites may provide links to a number of third-party websites. Please beware that we have no control over the manner in which these third party websites collect and process your personal data when you make use of them. When visiting those links, make sure you review first their privacy statements prior to providing any personal data to them.

2.4 Please note that our app (“Bancontact Pay”), available for download via links posted on our websites to Google Play and App Store, is covered by a specific Privacy Statement included in the app.

3. Personal data we may collect and process

3.1 When using our websites we may collect and process:

- data that you provide to us when you contact us via a contact form on our websites, such as:
 - first name and surname;
 - address;
 - phone number;
 - email address;
 - technical details about your device (i.e.: type of device, model, operating system);
 - Bancontact app token;
 - the content of your message;
 - the IP address you use when contacting us;
 - any other information you may choose to provide to us.
- data generated through automated technologies such as cookies, web beacons and similar technologies (*see section 4 below*).

3.2 Not all data that we collect and process constitute ‘*personal data*’. Personal data as defined by law refers to data which are related to an identified or identifiable natural person.

4. Use of cookies, web beacons and similar technologies

4.1 A cookie is a small (temporary) text file that our websites save on your computer or mobile device when you visit our websites. These cookies are used to save your preferences to be used during a later visit (e.g.: your choice of language). Additionally, cookies may also be used for marketing and remarketing purposes or to help protect our websites from spam and abuse by analysing traffic with the purpose of filtering the parts of traffic recognized as bots or spam and keep automated software from engaging in abusive activities on our websites.

A web beacon is a transparent graphic image, usually no larger than 1x1 pixels, used to monitor which web pages are visited on our websites. A web beacon is often used in combination with other cookies.

We may use cookies, web beacons and similar technologies in connection with our websites to monitor and analyze how the visitors make use of our websites. This information allows us to optimize visitors’ browsing experience and protect us from spam and abuse.

4.2 When we use cookies, web beacons and similar technologies in connection with our websites, we will use the functions available to us to allow collection of non-personal or anonymized data only. (For example, if we use Google Analytics, we will use the function available within Google Analytics for anonymizing your IP-address). Turning off your browser's cookies will prevent our web beacons from monitoring your activity on our websites. The web beacons will still account for your visit, but your unique information will be anonymous.

4.3 Our websites provide you with options for enabling/disabling different categories of cookies used on our websites. Currently our websites make use of functional cookies (strictly necessary for the good functioning of our websites), analytical cookies (related to determining how visitors use our websites), personalization cookies (used to enable improved functionality and customization of our websites) and marketing and remarketing cookies (used for optimizing our marketing campaigns based on the browsing behaviour of visitors on our websites).

We use the following cookies, tokens, trackers on our websites:

Cookie name	Type	Scope	Duration	Additional information
laravel_session	Essential / functional	Contains encrypted session information for the Laravel framework	1 hour	Laravel_session, XSRF-token and cookieConsent are from the PHP version that is running on our webserver called Laraval. The data from this cookie is stored locally on the server/PC and is not shared. Secure and encrypted Laravel cookies are where the sessions are stored
XSRF-token	Essential / functional	Contains a token to protect against cross-site request forgery (CSRF)	1 hour	Cross-site request forgery (also known as XSRF or CSRF) is an attack against web-hosted apps whereby a malicious web app can influence the interaction between a client browser and a web app that trusts that browser. These attacks are possible because web browsers send some types of authentication tokens automatically with every request to a website. This form of exploit is also known as a one-click attack or session riding because the attack takes advantage of the user's previously authenticated session.
cookieConsent	Essential / functional	Contains the consent provided by the user	1 year	Cookie Consent is a cookies management solution integrated in our websites which assists with the consent management as required under the EU Cookies Directive and the GDPR.

Friendly Captcha	Essential / functional	Prevents spam and blocks "bots": the program determines whether the user is a real person or a "bot" to stop "automated software" from weighing down our websites		
Google Ads	Marketing			Ad Settings helps control ads seen on Google services (such as Google Search or YouTube), or on non-Google websites and apps that use Google ad services. You can also learn how ads are personalized, opt out of ad personalization, and block specific advertisers: https://cookiedatabase.org/service/google-ads-optimization/
Google Analytical Cookies	Analytical			GOOGLE TERMS OF SERVICE (January 5th, 2022); GOOGLE PRIVACY POLICY (February 10, 2022)
YouTube (only if video is enabled)	Essential / functional	allowing viewing the on site available YouTube videos	6 months According to the applicable YouTube Privacy Policy	https://cookiedatabase.org/service/youtube/
Cloudflare	Essential / functional			
_ga	Functional	Used to distinguish users	2 years	Tracks user behavior on the Websites, which helps us better understand how users are using the Websites: 1/ _ga: to store and count pageviews. 2/ _gid: to store and count pageviews.

				3/ _gat: to read and filter requests from bots.
_gid	Functional	Used to identify/distinguish users;	24 hours	
_gat	Functional	Used to throttle request rate	1 minute	
Mixpanel	Analytical	Tracks specific user actions to help us understand how people interact with our features.	Session duration	
Hotjar	Analytical	Uses heatmaps and session recordings to improve website usability and user experience.	Session duration	
Facebook pixel	Marketing	Measures the effectiveness of our advertising and helps us serve relevant ads to you on Meta platforms.	180 days	
Google DV360	Marketing	An integrated tool that helps us manage programmatic ad campaigns and reach specific audiences across the web.	1,5 year	
Teads	Marketing	Native and outstream advertising platforms used to distribute our content and display ads across a network of	1 year	

		high-quality publishers.		
Zemanta	Marketing	Native and outstream advertising platforms used to distribute our content and display ads across a network of high-quality publishers.	1 year	

Additionally, you may also choose to configure your browser’s standard privacy and security settings, by installing certain browser specific add-ons (*such as “Google Analytics Opt-out Browser” add-on, which is currently available for most commonly used web browsers*). You may review these settings and change them prior to, or after you visit our websites. You may also choose to block or delete cookies. If you choose to change these settings after you have visited our websites (*e.g.: deleting all cookies*), next time you visit our websites you may be asked to consent again to our use of cookies, web beacons and similar technologies.

4.4 We have taken the necessary steps to ensure that the use of cookies on our websites is the least privacy intrusive as possible. However, depending on your choice for accepting or refusing cookies, you may or may not be able to use some or all of our websites’ features. Some cookies (such as session cookies) are essential for the proper functioning and displaying of our websites on your device but if you have chosen to disable all cookies in your browser settings, this will not be possible.

To optimize your visit to our websites, we recommend you review and accept our pre-existing cookie settings during your first visit. If you prefer not to, or you change your mind, you may always deactivate or modify the existing cookies settings, by accessing our cookie preference banner, via the dedicated link on the bottom of the webpage.

4.5 Additional information about browser settings and cookies could be found on <http://www.allaboutcookies.org/>.

5. Why do we process this data and for how long?

5.1 We process this data for a number of purposes:

- to allow you to use our websites and make it more convenient for you to do so;
For example, we may use the data by placing a cookie on your computer to remember your language preference for when you visit our websites again.
- to allow us to operate, maintain and optimize our websites and related systems;
For example, we may use the data to resolve technical issues surrounding our websites navigation and use.

- to ensure that our websites are used properly and securely;
For example, we may use the data to verify that we do not receive spam submissions through the contact form on our websites.
- to further develop and update our websites;
For example, we may use the data to analyze when and how visitors navigate on our websites. This helps us to understand what we need to change and improve on our websites and provide you with the best online experience.
- to communicate with you following your submission(s) via the contact form on our websites;
- for marketing purposes regarding our products and services;
For example: if you visit pages on our websites concerning the “Bancontact Pay” app, we may serve you with an add concerning our app via a social network you are a member of (e.g. Facebook).
- to enable us to comply with our obligations under applicable laws, the exercise or defense of legal claims, or to exercise our rights;
For example, we may need to process the data for evidence reasons.
- to allow you to register and use our “Bancontact Pay” app;
To find out how and why we collect and process your personal data when using our “Bancontact Pay” app, please refer to the Privacy Statement included in the app.
- other purposes for which you have given us your explicit and informed consent.

5.2 We retain your (personal) data for no longer than is necessary when using our products and services, except where we are under a legal obligation to retain your (personal) data longer.

6. Are we allowed to process your personal data?

6.1 We will process your (personal) data only to the extent allowed by the applicable data protection laws. Subject to the requirements of the applicable laws, we are permitted to process your (personal) data if:

- you have given us your consent to do so; and/or
- such processing is necessary for the performance of a contract or respond to requests you made to us (*e.g. to answer a question that you submitted through the online form on our website*); and/or
- the processing is necessary to pursue our legitimate interests or those of a third party;
(For example: we may for the purpose of optimizing our services and products, analyze how many times we are contacted concerning our “Bancontact Pay” app and what the nature of these contacts are)
- you are a registered user of our “Bancontact Pay” app.

6.2 Whenever your consent is required to allow us to process your personal data, we will inform you on the reason(s) for processing your data and will ask you beforehand whether you consent or not to such processing. You may choose not to consent. However, should you choose not to consent some features of our websites may not work properly and some functionality may not be available to you, or we may not be able to (fully) respond to your request.

6.3 We take appropriate security measures to prevent misuse and/or unauthorized access to your personal data. In doing so, we ensure that your personal data is kept safe and only our authorized personnel may access your data.

7. Do we share or transfer your personal data?

7.1 We do not share or transfer your personal data with any entity except:

- where you consented for us to do so; or
- to our service providers that are bound by contractual terms, as required by law, to allow processing on our behalf in accordance with this Privacy Statement; or
- if we are required to do so pursuant to law (*e.g. in response to a judicial or court order*); or
- to any entity that we acquire in whole or in part, or any entity that we are, in whole or in part, acquired by, merged into or merged with;
- as otherwise stated in this Privacy Statement or permitted by the applicable law(s).

7.2 We will not transfer your personal data outside of the European Economic Area unless:

- you have explicitly consented to the proposed transfer; or
- the transfer is strictly necessary for the conclusion or the performance of a contract concluded between you and us; or
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- an adequate level of protection of your personal data is ensured as determined by the European Commission; and
- appropriate safeguards are in place, as established by the European Commission.

8. Exercising your rights

8.1 The data protection laws that protect your personal data grants you certain rights. We will respect those rights and you may contact our DPO to exercise those rights.

8.2 Subject to the conditions stated under the GDPR and the Belgian Data Protection Act of 30 July 2018, you may:

- contact us requesting information on what personal data we have on you;
- rectify any erroneous personal data you (may) have submitted to us via our websites or via our app;
- 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 have questions with regard to this Privacy Statement or wish to exercise any of the above mentioned rights, you may do so by submitting an e-mail request to our [DPO](#). Alternatively, you may address your questions or exercise your rights by regular post at

Bancontact Company NV/SA
Aarlenstraat – Rue d’Arlon 82
1040 Brussels, Belgium

When you contact us, please be specific as to what information you require, or what right(s) 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. A response to your request shall be provided within the timeframe established by the applicable law(s).

If you believe that your rights with regard to the protection of your personal data are not upheld, you may submit a complaint to our DPO or, alternatively, you may choose to file your complaint with the [Belgian Data Protection Authority](#).

Last updated: 01/03/2026