Brave Corp

Privacy Policy

20TH MARCH 2023

BRAVE SECURITY CORPORATION S.L (hereinafter BraveCorp), with tax domicile in SPAIN and with N.I.F. B-01574870, is registered in the Registry of the Bank of Spain of providers of virtual currency exchange services and custody of virtual wallets with the number D764.

BraveCorp is the owner of the website: https://bravepay.net and the APP (iOS/Android) through which the services of the BravePay and BravePro Platform are accessed.

1. About this Policy

Brave Security Corporation S.L. ("us", "we", or "our") operates the BravePay web and mobile application (hereinafter referred to as the "Service").

This page informs you of our policies regarding the collection, use and disclosure of personal data when you use our Service and the choices you have associated with that data.

We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, the terms used in this Privacy Policy have the same meanings as in our Terms and Conditions.

Owner and Data Controller
Brave Security Corporation S.L
B Accelerator Tower
Gran Vía Don Diego López de Haro, 1
48001 Bilbao (Bizkaia)
Spain

Owner Contact e-mail
support@bravepay.net

2. Types of Data Collected

Among the types of Personal Data that this Application collects, by itself or through third parties, there are: Contacts permission; Camera permission; Cookies; Usage Data; email address; password.

Complete details on each type of Personal Data collected are provided in the dedicated sections of this privacy policy or by specific explanation texts displayed prior to the Data collection.
Personal Data may be freely provided by the User, or, in case of Usage Data, collected automatically when using this Application.

Unless specified otherwise, all Data requested by this Application is mandatory and failure to provide this Data may make it impossible for this Application to provide its services. In cases where this Application specifically states that some Data is not mandatory, Users are free not to communicate this Data without consequences to the availability or the functioning of the Service.

Users who are uncertain about which Personal Data is mandatory are welcome to contact the Owner.

Any use of Cookies – or of other tracking tools – by this Application or by the owners of third-party services used by this Application serves the purpose of providing the Service required by the User, in addition to any other purposes described in the present document and in the Cookie Policy, if available.
Users are responsible for any third-party Personal Data obtained, published or shared through this Application and confirm that they have the third party's consent to provide the Data to the Owner.

3. Mode and place of processing the Data

3.1 Methods of processing

The Owner takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Data.

The Data processing is carried out using computers and/or IT enabled tools, following organizational procedures and modes strictly related to the purposes indicated. In addition to the Owner, in some cases, the Data may be accessible to certain types of persons in charge, involved with the operation of this Application (administration, sales, marketing, legal, system administration) or external parties (such as third-party technical service providers, mail carriers, hosting providers, IT companies, communications agencies) appointed, if necessary, as Data Processors by the Owner. The updated list of these parties may be requested from the Owner at any time.

3.2 Legal basis of processing

The Owner takes appropriate security measures to The Owner may process Personal Data relating to Users if one of the following applies:

- Users have given their consent for one or more specific purposes. Note: Under some legislations the Owner may be allowed to process Personal Data until the User objects to such processing ("opt-out"), without having to rely on consent or any other of the following legal bases. This, however, does not apply, whenever the processing of Personal Data is subject to European data protection law;
- provision of Data is necessary for the performance of an agreement with the User and/or for any pre-contractual obligations thereof;
- processing is necessary for compliance with a legal obligation to which the Owner is subject;
- processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Owner;

- processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Owner;
- processing is necessary for the purposes of the legitimate interests pursued by the Owner or by a third party.

In any case, the Owner will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

3.3 Legal Basis for Processing Personal Data under the General Data Protection Regulation (GDPR)

If you are from the European Economic Area (EEA), Brave Security Corporation S.L. legal basis for collecting and using the personal information described in this Privacy Policy depends on the Personal Data we collect and the specific context in which we collect it. Brave Security Corporation S.L. may process your Personal Data because:

- We need to perform a contract with you
- You have given us permission to do so
- The processing is in our legitimate interests and it is not overridden by your rights
- For payment processing purposes
- To comply with the law

3.4 Place

The Data is processed at the Owner's operating offices and in any other places where the parties involved in the processing are located.

Depending on the User's location, data transfers may involve transferring the User's Data to a country other than their own. To find out more about the place of processing of such transferred Data, Users can check the section containing details about the processing of Personal Data.
Users are also entitled to learn about the legal basis of Data transfers to a country outside the European Union or to any international organization governed by public international law or set up by two or more countries, such as the UN, and about the security measures taken by the Owner to safeguard their Data.

If any such transfer takes place, Users can find out more by checking the relevant sections of this document or inquire with the Owner using the information provided in the contact section.

3.5 Retention Time

Personal Data shall be processed and stored for as long as required by the purpose they have been collected for.

Therefore:

- Personal Data collected for purposes related to the performance of a contract between the Owner and the User shall be retained until such contract has been fully performed.
- Personal Data collected for the purposes of the Owner's legitimate interests shall be retained as long as needed to fulfill such purposes. Users may find specific information regarding the legitimate interests pursued by the Owner within the relevant sections of this document or by contacting the Owner.

The Owner may be allowed to retain Personal Data for a longer period whenever the User has given consent to such processing, as long as such consent is not withdrawn. Furthermore, the Owner may be obliged to retain Personal Data for a longer period whenever required to do so for the performance of a legal obligation or upon order of an authority.

Once the retention period expires, Personal Data shall be deleted. Therefore, the right of access, the right to erasure, the right to rectification and the right to data portability cannot be enforced after expiration of the retention period.

Brave Security Corporation S.L. will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of our Service, or we are legally obligated to retain this data for longer periods.

4. The purposes of processing

Brave Security Corporation S.L. uses the collected data for various purposes:

- To provide and maintain our Service
- To comply with its legal obligations
- To respond to enforcement requests
- To protect its rights and interests (or those of its Users or third parties)
- To detect any malicious or fraudulent activity
- To notify you about changes to our Service
- Device permissions for Personal Data access
- Registration and authentication

- Registration and authentication
- Access to third-party accounts
- Registration and authentication provided directly by this Application
- To allow you to participate in interactive features of our Service when you choose to do so
- To provide customer support
- To gather analysis or valuable information so that we can improve our Service
- To monitor the usage of our Service
- To detect, prevent and address technical issues

For specific information about the Personal Data used for each purpose, the User may refer to the section “Detailed information on the processing of Personal Data”.

5. Device permissions for Personal Data access

Depending on the User's specific device, this Application may request certain permissions that allow it to access the User's device Data as described below.

By default, these permissions must be granted by the User before the respective information can be accessed. Once the permission has been given, it can be revoked by the User at any time. In order to revoke these permissions, Users may refer to the device settings or contact the Owner for support at the contact details provided in the present document.
The exact procedure for controlling app permissions may be dependent on the User's device and software.

Please note that the revoking of such permissions might impact the proper functioning of this Application.

If User grants any of the permissions listed below, the respective Personal Data may be processed (i.e accessed to, modified or removed) by this Application.

5.1 Approximate location permission (continuous)

We may use and store information about your location if you give us permission to do so ("Location Data"). We use this data to provide features of our Service, to improve and customise our Service (e.g. Determine the legal age applicable in a given location to access to certain products). You can enable or disable location services when you use our Service at any time by way of your device settings

5.2 Camera Permission

Used for accessing the camera or capturing images and video from the device.

5.3 Contacts permission

Used for accessing contacts and profiles on the User's device, including the changing of entries.

6. Detailed information on the processing of Personal Data

Personal Data is collected for the following purposes and using the following services:

6.1 Access to third party accounts

This type of service allows this Application to access Data from your account on a third-party service and perform actions with it.

These services are not activated automatically, but require explicit authorization by the User.

6.2 Analytics

The services contained in this section enable the Owner to monitor and analyze web traffic and can be used to keep track of User behavior.

Google Analytics

Google Analytics is a web analysis service provided by Google LLC or by Google Ireland Limited, depending on the location this Application is accessed from, (“Google”). Google utilizes the Data collected to track and examine the use of this Application, to prepare reports on its activities and share them with other Google services.

Google may use the Data collected to contextualize and personalize the ads of its own advertising network.

Personal Data processed: Cookies; Usage Data.

Place of processing: United States – Privacy Policy – Opt Out; Ireland – Privacy Policy – Opt Out.

6.3 Registration and authentication

By registering or authenticating, Users allow this Application to identify them and give them access to dedicated services.

Depending on what is described below, third parties may provide registration and authentication services. In this case, this Application will be able to access some Data, stored by these third-party services, for registration or identification purposes.

Some of the services listed below may also collect Personal Data for targeting and profiling purposes; to find out more, please refer to the description of each service.

Google OAuth

Google Ireland Limited, depending on the location this Application is accessed from, and is connected to the Google network.

Personal Data processed: various types of Data as specified in the privacy policy of the service.

Place of processing: United States – Privacy Policy; Ireland – Privacy Policy.

6.4 Device permissions for Personal Data access

This Application requests certain permissions from Users that allow it to access the User's device Data as described below.

Device permissions for Personal Data access (this Application)

This Application requests certain permissions from Users that allow it to access the User's device Data as summarized here and described within this document.

Personal Data processed: Approximate location permission (continuous); Camera permission; Contacts permission.

6.5 Registration and authentication provided directly by this Application

By registering or authenticating, Users allow this Application to identify them and give them access to dedicated services. The Personal Data is collected and stored for registration or identification purposes only. The Data collected are only those necessary for the provision of the service requested by the Users.

Direct registration (this Application)

The User registers by filling out the registration form and providing the Personal Data directly to this Application.
Personal Data processed: email address; password, date of birth, picture, ID or Passport, bank card details, bank account details, company registration details.

7. Transfer of Data

Your information, including Personal Data, may be transferred to - and maintained on - computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ from those of your jurisdiction. If you are located outside Spain and choose to provide information to us, please note that we transfer the data, including Personal Data, to Spain and process it there.

Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer. Brave Security Corporation S.L. will take all the steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

8. Disclosure of Data

8.1 Business Transaction

If Brave Security Corporation S.L. is involved in a merger, acquisition or asset sale, your Personal Data may be transferred. We will provide notice before your Personal Data is transferred and becomes subject to a different Privacy Policy.

8.2 Disclosure of law enforcement

Under certain circumstances, Brave Security Corporation S.L. may be required to disclose your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

8.3 Legal requirements

Brave Security Corporation S.L. may disclose your Personal Data in the good faith belief that such action is necessary to:

- To comply with a legal obligation
- To protect and defend the rights or property of Brave Security Corporation S.L.
- To prevent or investigate possible wrongdoing in connection with the Service
- To protect the personal safety of users of the Service or the public
- To protect against legal liability

9. Security of Data

The security of your data is important to us but remember that no method of transmission over the Internet or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

10. Our Policy on "Do Not Track" Signals under the California Online Protection Act (CalOPPA)

We do not support Do Not Track ("DNT"). Do Not Track is a preference you can set in your web browser to inform websites that you do not want to be tracked.

You can enable or disable Do Not Track by visiting the Preferences or Settings page of your web browser.

11. The rights of the users

Users may exercise certain rights regarding their Data processed by the Owner.
In particular, Users have the right to do the following:

- **Withdraw their consent at any time.** Users have the right to withdraw consent where they have previously given their consent to the processing of their Personal Data.
- **Object to processing of their Data**. Users have the right to object to the processing of their Data if the processing is carried out on a legal basis other than consent. Further details are provided in the dedicated section below.
- **Access their Data.** Users have the right to learn if Data is being processed by the Owner, obtain disclosure regarding certain aspects of the processing and obtain a copy of the Data undergoing processing.
- **Verify and seek rectification.** Users have the right to verify the accuracy of their Data and ask for it to be updated or corrected.
- **Restrict the processing of their Data.** Users have the right, under certain circumstances, to restrict the processing of their Data. In this case, the Owner will not process their Data for any purpose other than storing it.
- **Have their Personal Data deleted or otherwise removed.** Users have the right, under certain circumstances, to obtain the erasure of their Data from the Owner.
- **Receive their Data and have it transferred to another controller**. Users have the right to receive their Data in a structured, commonly used and machine readable format and, if technically feasible, to have it transmitted to another controller without any hindrance. This provision is applicable provided that the Data is processed by automated means and that the processing is based on the User's consent, on a contract which the User is part of or on pre-contractual obligations thereof.
- **Lodge a complaint.** Users have the right to bring a claim before their competent data protection authority.

Details about the right to object to processing

Where Personal Data is processed for a public interest, in the exercise of an official authority vested in the Owner or for the purposes of the legitimate interests pursued by the Owner, Users may object to such processing by providing a ground related to their particular situation to justify the objection.

Users must know that, however, should their Personal Data be processed for direct marketing purposes, they can object to that processing at any time without providing any justification. To learn, whether the Owner is processing Personal Data for direct marketing purposes, Users may refer to the relevant sections of this document.

12. Service Providers

We may employ third party companies and individuals to facilitate our Service ("Service Providers"), provide the Service on our behalf, perform Service-related services or assist us in analyzing how our Service is used. These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

12.1 Analytics

We may use third-party Service Providers to monitor and analyse the use of our Service.

Firebase

Firebase is an analytics service provided by Google Inc.
You may opt-out of certain Firebase features through your mobile device settings, such as your device advertising settings or by following the instructions provided by Google in their Privacy Policy.

We also encourage you to review the Google's policy for safeguarding your data.

For more information on what type of information Firebase collects, please visit the Google Privacy & Terms web page.

12.2 Payments

We may provide paid products and/or services within the Service. In that case, we use third-party services for payment processing (e.g. payment processors). We will not store or collect your payment card details. That information is provided directly to our third-party payment processors whose use of your personal information is governed by their Privacy Policy. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, MasterCard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

The payment processors we work with are:

Apple Store In-App Payments
Their Privacy Policy can be viewed here

Google Play In-App Payments
Their Privacy Policy can be viewed here

Stripe
Their Privacy Policy can be viewed here

PayPal / Braintree
Their Privacy Policy can be viewed here

FastSpring
Their Privacy Policy can be viewed here

Authorize .net
Their Privacy Policy can be viewed here

2Checkout
Their Privacy Policy can be viewed here

SagePay
Their Privacy Policy can be viewed here

Square
Their Privacy Policy can be viewed here

Go Cardless
Their Privacy Policy can be viewed here

Elavon
Their Privacy Policy can be viewed here

Verifone
Their Privacy Policy can be viewed here

Wechat
Their Privacy Policy can be viewed here

AliPay
Their Privacy Policy can be viewed here

12.3 Identity verification

For AML purposes, we may use third-party Service Providers to assess the authenticity of official documents and verify the age and identity of the users.

ID Analyzer
Their Privacy Policy can be viewed here

13. Links to other sites

Our Service may contain links to other sites that are not operated by us. If you click a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit. We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

14. Children’s privacy

Our Service does not address anyone under the age of 14 (“Children”).

We do not knowingly collect personally identifiable information from anyone under the age of 14. If you are a parent or guardian and you are aware that your

Child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers. ur Service may contain links to other sites that are not operated by us. If you click a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit. We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

15. Changes in this policy

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page. We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

16. Contact us

If you have any questions about this Privacy Policy, please contact us:

By email: support@BravePay.net