

Privacy Notice for Brite's services

Last update: 22 January 2026

Welcome to our Privacy Notice for Brite's services!

Thank you for using our website and services.

Here you will find information about:

- **what** personal data we process about you,
- **why** and **how** we do it,
- **where** it came from,
- **who** is involved and with **whom** we may share it with, and
- **how** it is lawful for us to do it.

Personal integrity is important to us, and we take your privacy seriously. We encourage you to read this Privacy Notice. We hope it can help you make informed decisions. By reading this Privacy Notice we hope you feel confident that we work hard to live up to your expectations.

We may provide this Privacy Notice in languages other than English. If there are any discrepancies between other language versions and the English language version, the English version is authoritative.

Please contact us if you have any questions regarding this Privacy Notice or questions in general regarding your personal data. You can always contact us by sending an email to dataprotection@britepayments.com.

1. About us

Brite AB, corporate registration number 559116-1632, with registered address at Linnégatan 5, 114 47 Stockholm, Sweden ('**Brite**', '**we**', '**us**'), is a payment service provider that provides payment services including payment initiation services and account information services (the '**Services**'). Brite is licensed by and subject to the supervision of the Swedish Financial Supervisory Authority (Sw. *Finansinspektionen*).

In connection with these services, the following Brite group companies also act as a data controller and process your data in accordance with this Privacy Notice:

- Brite AB Sucursal En España, W0267281D, Spain,
- Brite AB Malta Branch, OC 1500, Malta,
- Brite AB Succursale Française, 928 009 794 R.C.S, France, and
- Brite AB Zweigniederlassung HRB 24483B, Germany.

Any reference made to '**Brite**', '**we**', '**us**', '**Brite group companies**' included in this Privacy Notice shall mean the group of companies which directly or indirectly controls, is controlled by, or is under common control with us.

2. Our role

In this Privacy Notice we describe what personal data we collect and process of you as an 'End-user' and an individual that contacts our support via our support channels such as our website.

End-users

Brite is the data controller for the processing of your personal data when you use our payment services, or any related services provided by us, for payments to or from our merchants ('End-user', 'you').

Please note that your payment account provider (normally the bank where you hold the account used for payment transactions initiated through Brite) and the merchant you are transacting with or partner you are interacting with, are separate and independent controllers for the processing of personal data in connection with the products and/or services they provide to you and their business activities. **Please contact them directly for information on their processing of your personal data.**

"Merchant" shall be understood as the business that provides a product or services to you and that uses Brite as a payment option online.

"Partner" means businesses that are themselves regulated payment service providers who use us as their online payment solution for the purpose of executing payments for the benefit of their own customers (sub-merchants) or to collect financial information through the use of the Account Information Service from end-users for the benefit of their own customers (sub-merchants).

Website visitors

We are also the data controller for personal data processed when someone uses our website or otherwise contacts us through our support channels.

3. Who to contact?

You are welcome to contact us at dataprotection@britepayments.com if you have any questions about this Privacy Notice, our use of your personal data or if you wish to exercise your rights.

Brite AB has appointed Bird&Bird DPO Services SRL, as its data protection officer and the data protection officer can be contacted through the following channels:

- via email: dpo@britepayments.com
- by post: Bird & Bird DPO Services SRL, Avenue Louise 235 b 1, 1050 Brussels, Belgium.

4. Your rights

You have several rights relating to the processing of your personal data.

You are entitled to receive information about what personal data we use about you and what we do with this data and also, to a certain extent, to check your data. You are thus entitled in certain cases to receive data or have it rectified, erased, blocked, or moved. You are also entitled to object to certain kinds of use of your data or revoke your consent to it being used. You are always entitled to file a complaint with the Swedish Authority for Privacy Protection or the data protection authority in your homeland if you think that we have used your data in an unpermitted way.

You can find out more about your rights under each heading below. Please note that there are exceptions to the rights below, so access may be denied, for example where we are legally prevented from making a disclosure.

You can contact us at any time if you wish to exercise your rights by contacting us on dataprotection@britepayments.com.

Our responsibility for your rights

We are obliged to respond to your request to exercise your rights within one (1) month from being contacted by you. We are entitled to extend this period by a further two (2) months if your request is complicated or if we have had a large number of enquiries.

If we consider that we cannot do what you want us to do, we are obliged to notify you, no later than within one (1) month from receipt of your request, of why we cannot do what you want us to do and inform you that you are entitled to file a complaint with the supervisory authority.

All information, communication, and all of the measures that we implement are free of charge for you. However, we are entitled to levy an administrative charge to provide you with the information or implement the measure requested, or to refuse to accommodate your request, if what you have asked is manifestly unfounded or unreasonable.

Right to be informed

You have the right to be informed of how we process your personal data. We do this through this Privacy Notice, by service-specific FAQs, and by answering your questions.

Right of access

You are entitled to ask for a register extract relating to our use of your personal data. You are also entitled to receive a copy of the personal data that we use free of charge. We are entitled to levy an administration charge for any additional copies. If you make a request in an electronic format (e.g. by email), we will give you the information in a commonly used electronic format.

Right to rectification

We will, at your request or on our own initiative, rectify, de-identify, erase or supplement data that we discover to be inaccurate, incomplete or misleading. You are also entitled to supplement it with additional data if anything of relevance is missing.

Right to erasure

You are entitled to ask us to remove your personal data if there are no longer any acceptable reasons for us to use it. The data shall therefore be erased if:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed,

- we are using your data on the basis of your consent and you revoke this and there is no other legal ground for the processing,
- you object to our use of your data which has been used following a balance of interests and we do not have important interests that override your interests or rights,
- you object to our use of your personal data for the purposes of direct marketing,
- we have used the personal data in an unpermitted way,
- we have a legal obligation to erase the personal data, or
- you are a child and we have collected the personal data in conjunction with an offer of information society services.

However, there may be a statutory requirement or other substantially compelling reason that means that we cannot immediately erase your personal data. We will then stop using your personal data for purposes other than to comply with legislation or that are not necessary for any other substantially compelling reason.

Right to restriction of processing

You are entitled to request restriction of our processing when:

- you consider that your data is inaccurate and you have requested rectification, during the period when we are investigating the accuracy of the data,
- the use is unlawful and you do not wish to have the data erased,
- we, as controllers, no longer need the personal data for our purposes of use, but you need it to be able to establish, exercise or defend a legal claim, or
- you have objected to its use, pending a check about whether our important interests outweigh your interests.

Right to object

You are entitled to object to such use of your personal data that we do on the basis of a balance of interests or a general interest. If you object to such use, we will only continue to use the data if we have important reasons to continue to use it that outweigh your interests.

Right to data portability

You have a right to data portability. This means a right to receive some of your personal data in a structured, commonly used and machine-readable format and be able to transfer this data to another controller. You only have a right to data portability when the use of your personal data is automated and we base our use on your consent or on a contract between you and us. This means that you, for example, are entitled to receive and transfer all of the personal data input by you to create your user account with us.

Right to object to automated decision making

You have the right to object to an automated decision made by us, if the automated decision produces legal effects or similarly significantly affects you. Please read more under section 12 in this Privacy Notice.

Right to withdraw your consent

In cases where we process your personal data based on your consent, you have the right to withdraw your consent with **prospective effect** (either partially or completely) at any time by sending an email to dataprotection@britepayments.com.

Your withdrawal of consent does not affect the lawfulness of the personal data processing that was performed based on your consent before you withdrew your consent.

Your right to complain to a supervisory authority

You are entitled to lodge a complaint about our processing of your personal data to the Swedish Authority for Privacy Protection, which is the supervisory authority for Brite. You can also file a complaint with the data protection authority in your homeland within the EU.

5. What personal data do we collect and process about you?

- **Identifying information:** name (first and last name), personal identity (ID) number, date of birth, postal address, gender, email address, phone number, nationality, citizenship, age, copies of and information from your ID documents such as passport or ID card.
- **Financial information and other identifying information:** sending and/or receiving bank, IBAN, bank account number, name of account, bank account ownership, source of funds and amounts related thereto, proof of funds, account balance at the time of payment, account information such as account history, information about credits, information about purchases (such as amount, time, type of transaction and in some cases type of goods and/or place of purchase), and other financial information derived from your accounts, information identifying an end-user's payment such as order id, message id, payment reference id, transaction id and the time when the transaction was made, and customer id identifying you as a user in our system. The IDs that identify you and your payment are generated in our systems when you use our service.
- **Behaviour information:** how you use our payment service and/or how website visitors interact with our websites.
- **Work related data:** such as employer and title.
- **Geographical information:** County, country.
- **Transaction and correspondence history.**
- **Device data:** such as IP-number, type of device, operating system and browser information.
- **Information related to your contacts with our customer service:** information provided by you through our contact form on our website, and email correspondence.
- **Information from external sanction lists and PEP/RCA lists:** sanction lists and lists of persons constituting politically exposed persons ("PEP") or relatives and close associates of PEP ("RCA") include information such as name, date of birth, place of birth, occupation or position, and the reason why the person is on the list in question.

6. Why do we process your personal data?

We process your personal data so that we can, in the best possible way, provide you with the services we offer for the following overall purposes. More information is provided under each purpose that you can read to find about, among other things, what personal data we use to achieve the purpose, the way in which we use the personal data and how long we will process the personal data for the purpose in question.

Your personal data is used for the following overall purposes, which are further explained below:

- For the provision of our services to you.
- For the administration and provision of support and customer services to you.
- To enable us to perform Customer Due Diligence (CDD), Enhanced Due Diligence (EDD) checks and Ongoing Due Diligence (ODD) and to fulfil our legal obligations.
- Administration in conjunction with corporate acquisitions, restructuring, etc.
- To defend and attend to legal claims.
- To market and sell our services to you.

We do not use your personal data for any other incompatible purpose.

Providing us with your personal data is voluntary, but necessary to enable you to use our service. It will not be possible to execute payments if you do not provide personal data.

Administration and provision of our services to you

What we do

We process the following personal data about you to enable us to execute payments initiated by you, and also to be able to provide and administer our services in accordance with our conditions of use. This includes, for example, verifying that you are over such age that is allowed for the access to the Services and identifying you before a transaction is executed. We obtain the following information to enable us to determine the identity of our users, contact them if required, and also the financial information required to be able to provide the services.

Personal data

- Identifying information: name (first and last name), e-mail, phone number, personal identity (ID) number, date of birth, postal address, gender, nationality, citizenship, age.
- Financial information and other identifying information: sending and/or receiving bank, IBAN, bank account number, name of account, bank account ownership, account balance at the time of payment, account information such as account history, information about credits, information about purchases (such as amount, time, type of transaction and in some cases type of goods and/or place of purchase), and other financial information derived from your accounts, information identifying an end-user's payment such as order id, message id, payment reference id, transaction id and the time when the transaction was made, and customer id identifying you as a user in our system. The IDs that identify you and your payment are generated in our systems when you use our service.
- Transaction and correspondence history.
- Behaviour information: how you use our payment service.

- Geographical information: County, country.
- Device data: such as IP-number, type of device, operating system and browser information.
- Any other information provided to us by you.

Legal basis

We are entitled to use your data to perform our contract with you.

Storage period

Two (2) years from when Brite's service was last used. The data may be saved for longer if it is required to establish, defend, or exercise a legal claim or for the duration of the contractual relationship and thereafter for a maximum of ten (10) years based on statutes of limitations. Data that Brite has a legal obligation to retain under bookkeeping laws is generally retained for 7 years.

Administration and provision of support and customer services to you

What we do

We process your personal data in order to provide administrative support if you for example contact us with any questions regarding our services through any channel. Such contact may occur through e.g. e-mail to one of our specified e-mail addresses, through our chatbox or through the contact forms on our website.

You have the right to object to processing of your personal data based upon a legitimate interest as legal basis. Please see section 4 for more information about your rights.

Personal data

- Identifying information: name, e-mail, phone number.
- Work related data, such as employer and title.
- Geographical information: County, country.
- Transaction and correspondence history.
- Financial information and other identifying information: IDs that identify you and your payment in our systems such as customer ID, payment reference ID, proof of payment documentation, and IBAN.
- Device data, such as IP-number.
- Any other information provided to us by you.

Legal basis

After a balancing of interests, we have assessed that Brite's interest of processing your personal data in order to administer the provision of our support and customer services overrides your interest of protection of your privacy. Hence, the legal basis is legitimate interest.

Storage period

Two (2) years from the date when Brite collected your data or the date when you last contacted us, whichever is later. The data may be saved for longer if it is required to establish, defend or exercise a legal claim.

To market and sell our services to you

What we do

We process your personal data to market Brite and our services. We may use your data to e.g. send our newsletter or directly contact you after the completion of one of our forms on our website (www.britepayments.com). The purpose of our marketing measures is to send you direct advertisements as well as to contact you with information about our services.

You have the right to object to processing of your personal data based upon a legitimate interest as legal basis. When our processing of your personal data is based on your consent, you have the right to withdraw your consent at any time. Moreover, you can easily opt-out from any direct marketing performed by Brite, e.g. if we send our newsletter to you. Information on how to opt-out will be provided in each communication to you and is further explained in section 4 below, together with more information regarding your rights.

Personal data

- Identifying information: name, e-mail and phone number.
- Work related data, such as employer and title.
- Financial information: Account information.
- Device data, such as IP-number.
- Any other information provided to us by you.

Legal basis

After a balancing of interests, we have assessed that Brite's interest of offering its product and services that meet the needs and desires of its customers overrides your interest of protection of your privacy. Hence, the legal basis is legitimate interest.

In relation to direct marketing, we base our processing on your consent.

Storage period

Two (2) years from the date when Brite collected your data or the date when you last contacted us, whichever is later. You may at any time object to our processing of your personal data for the purpose of direct marketing. If you object, you will no longer receive direct marketing. For more information about your rights, see section 4.

To enable us to perform Customer Due Diligence ('CDD'), Enhanced Customer Due Diligence ('EDD') checks and Ongoing Due Diligence ('ODD') checks and to fulfil our legal obligations

What we do

We process the following personal data about you to enable us to perform CDD and EDD and ODD checks as applicable, including anti-money-laundering checks and checks against sanctions and PEP/RCA lists.

We may also be required to report statistics to authorities on inter alia fraudulent transactions and report suspicious payments to the police or similar authorities.

Personal data

- Identifying information: Name, personal identity (ID) number, date of birth, postal address, gender, nationality, citizenship, age, copies of and information from your ID documents such as passport and ID card.
- Financial information and other identifying information: Account information, source of funds and amounts related thereto and customer-ID.
- Information from external sanction lists and PEP/RCA lists: sanction lists and lists of persons constituting politically exposed persons ("PEP") and relatives and close associates to PEP ("RCA") include information such as name, date of birth, place of birth, occupation or position, and the reason why the person is on the list in question.

Legal basis

We have a legal obligation in accordance with the Measures against Money Laundering and Terrorism Financing Act (2017:630) to perform these checks. To the extent the information constitutes sensitive information, the legal basis is necessary for reasons of public interest (article 9(2)(g) GDPR). The sensitive information may contain e.g., information about political opinion in PEP/RCA lists.

Storage period

Your personal data will be processed for this purpose as a minimum for five (5) years and for up to ten (10) years following the date of termination of the relationship for the purpose of preventing, detecting, and investigating money laundering, terrorist financing and fraud, in accordance with legal requirements set out in the Measures against Money Laundering and Terrorism Financing Act (2017:630).

Administration in conjunction with acquisitions, restructuring, etc.

What we do

If Brite were to be restructured, for example split into several different operations, or if an external party were to acquire Brite or parts of our operation, Brite will transfer your personal data together with the personal data of other users to the acquiring company. This company will, in such cases, continue to use your personal data for the same purposes as specified by us in this Privacy Notice unless you receive other information in conjunction with the transfer.

Personal data

All of the personal data we process about you in accordance with this Privacy Notice, with the exception of sensitive personal data that will not be transferred, might be processed for this purpose depending on the circumstances.

Legal basis

We are entitled to use your data on the basis of a balance of interests as we consider that our interest in facilitating an acquisition or restructuring process outweighs your interest in protecting your personal data. However, a precondition for this is that the acquiring company conducts an operation similar to Brite.

Storage period

If Brite ceases to exist (e.g., owing to a merger, liquidation or bankruptcy), we will erase your personal data unless we need to save it in order to fulfil statutory requirements.

If Brite is bought by an acquiring company or is split up in conjunction with restructuring, we will continue to save and use your personal data in accordance with the provisions of this Privacy Notice, unless you receive other information in conjunction with the transfer.

Defend and deal with legal claims

What we do

If a dispute arises, we are entitled to use your data for the purpose of establishing, defending, or exercising the legal claim.

Personal data

- All of the personal data we process about you in accordance with this Privacy Notice might be processed for this purpose depending on the circumstances.

Legal basis

We are entitled to use your data on the basis of a balance of interests.

Storage period

The data is saved for the entire contractual relationship and for up to twelve (12) months following termination of the contract. The data may be saved for longer if it is required to establish, defend, or exercise a legal claim or for the duration of the contractual relationship and thereafter for a maximum of ten (10) years based on statutes of limitations.

7. How do we collect your personal data?

When you use our service and interact with us, we collect your personal data. This is where we describe from what sources we may collect your personal data.

From what sources do we collect your data?	How do we use your personal data?
<i>From you directly</i>	We collect your personal data mainly from you directly when you use our service.
<i>From third party service providers and sources</i>	<p>We may use a third party to collect your personal data.</p> <p>The personal data we collect from a third party may include forename, surname, address, date of birth, personal identity (ID) number, email address, gender, information about source of funds and amounts related thereto and transaction history.</p> <p>Data is collected from a third party when you use Brite's payment client or as part of the transaction monitoring as applicable.</p> <p>We will also screen you against PEP/RCA and sanctions lists which entails that we may receive data about you from the provider that we use for such purposes.</p> <p>The third parties we use depend on the country in which you are registered in the population register.</p> <p>We use the following third-party suppliers to obtain data about you:</p> <p>DevCode Identity AB, corporate registration number 559134-1960, Sveavägen 49, 113 59 Stockholm, Sweden</p> <p>Roaring Apps AB - corporate registration number 559067-2613, Propellervägen 4, 183 62, Täby, Sweden</p> <p>Suomen Asiakastieto Oy - corporate registration number 0111027-9, Hermannin rantatie 6, Box 16, 00581 Helsinki, Finland</p> <p>Finnish Trust Network (FTN) through Telia Finland Oyj – corporate registration number 1475607-9, Teollisuuskatu 15, 00510 Helsinki, Finland</p>

	<p>Softtronic CM1 AB - corporate registration number 559382-6505, SE-120 32, Stockholm, Sweden</p> <p>Statens personadressregister ("SPAR")</p>
<i>From the merchant or partner</i>	<p>We may collect personal data from the merchant from which you buy goods or services or the partner you interact with.</p> <p>An example would be your bank account number to which you want to receive payments to or from your merchant or partner or identifying information such as name, date of birth, address and IDs identifying you in our systems.</p>
<i>From your bank</i>	<p>We may collect your personal data from your online banking interface (i.e., online bank) or via an API provided by your bank. The provision of our services may thus require us to collect information from your bank regarding bank accounts, account transactions and other financial information.</p>

8. To whom do we disclose your personal data?

The personal data we collect about you may be shared with different categories of recipients depending on for what purpose we collected your data.

In this section, you can read more about the sharing we do of personal data belonging to you as an End-user using our payment service, and any other service provided by us to you, and as a web-site visitor.

8.1 If you are an End-User

8.1.1 Your merchant

Description of recipient	Purpose and legal ground
<p>For your merchant verifying payments in order to be able to e.g., release any purchased goods, we provide the merchant with information on the payments.</p> <p>Identifying information and/or financial information may also be shared with your merchant if the merchant is legally obliged to verify your identity as a measure to prevent money laundering, fraud, or other criminal act</p>	<p>We may share your personal data with the merchant on the basis that this is necessary for us to fulfil our contractual obligations as well as our legitimate interest to carry out the transaction and the merchant's legitimate interest or legal obligation of verifying payments and/or your identity.</p> <p>Our legitimate interest in sharing your personal data with your merchant is sometimes also</p>

<p>or to meet other potential legal and/or regulatory requirements imposed on the merchant.</p> <p>We may also share your personal data if the merchant has a legitimate interest to verify your identity or financial information or that you indeed are the actual holder of a bank account.</p>	<p>based on your wish to share your personal information to your merchant in order for you to verify your bank account, identity and/or use your merchant's service.</p> <p>The legal basis for sharing data with the merchant is therefore:</p> <ul style="list-style-type: none"> • partly the performance of a contract, Article 6(1)(b) of the GDPR, insofar as the data sharing takes place to perform the contract between you and the merchant, and • partly the legitimate interest of the merchant and ourselves, Article 6(1)(f) of the GDPR.
<p>If one of our contracted merchants' merges, sell, or otherwise restructure a company for which we are contractually obligated to provide our Services, we may share your personal data, in accordance with the purposes set out in this section, with the acquiring merchant which takes over the contract with us as part of such merge, acquisition or restructure.</p>	<p>The sharing in the case one of our contracted merchants' merges, sell or otherwise restructure its company is carried out on the basis that it is necessary for us to fulfil our contractual obligations as well as our legitimate interest to carry out the transaction and the merchant's legitimate interest or legal obligation of verifying payments and/or your identity.</p>

8.1.2 Partners

Description of recipient	Purpose and legal ground
<p>We may share your personal data, such as identifying information and financial information, with partners who enable their customers (sub-merchants) to integrate our services into their app or website. You choose these partners when you interact with them on the sub-merchant's webpage or app, and you choose to use our services for their benefit, e.g., if you choose to use our payment initiation service on the sub-merchant's website for the benefit of such sub-merchant, but where the payment is made to the partner, or if you choose to use our account information service</p>	<p>Your personal data is shared with the partner you chose so that this partner can perform and manage its relationship with you, for example by confirming your identity, sending goods, handling questions and disputes, preventing fraud, and where applicable.</p> <p>The partner's or sub-merchant's privacy notice, as applicable, applies to the processing of your personal data that has been shared with the partner or sub-merchant and that the partner or sub-merchant processes. Normally, you will</p>

<p>on such sub-merchant's website or app.</p>	<p>find a link to the partner's or sub-merchant's privacy notice on the partner's or sub-merchant's website.</p> <p>We may share your personal data with the partner based on the fact that it is necessary for us to fulfil our contractual obligations as well as our legitimate interest in carrying out the transaction and the partner's legitimate interest or legal obligation to verify payments and/or your identity.</p> <p>Our legitimate interest in sharing your personal data with your partner is sometimes also based on your wish to share your personal information with your partner so that you can verify your bank account, your identity, and/or use your partner's service.</p> <p>The legal basis for sharing data with partners is thus:</p> <ul style="list-style-type: none"> • partly the performance of a contract, Article 6(1)(b) of the GDPR, insofar as the data sharing takes place to perform the contract between you and the partner, and • partly the legitimate interest of the partner and ourselves, Article 6(1)(f) of the GDPR. <p>We ensure that the processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have your information processed for this purpose.</p> <p>You have the right to object to this processing based on legitimate interest, for reasons connected to the circumstances in your particular case.</p> <p>You can contact us to learn more about our determination in your case, see section 4 for contact details and see section 5 for more information about your rights.</p>
<p>If one of our contracted partners merges, sells,</p>	<p>The sharing in the event that one of our</p>

or otherwise restructures a company for which we are contractually obligated to provide our services, we may share your personal data, in accordance with the purposes stated above, with the acquiring partner that takes over the contract with us as part of such merger, acquisition, or restructuring.	contracted partners merges, sells, or otherwise restructures its business is performed on the basis that it is necessary for us to fulfill our contractual obligations as well as our legitimate interest in executing the transaction and the partner's legitimate interest or legal obligation to verify payments and/or your identity.
---	---

8.1.3 Sharing account information with our partners or merchants when you use our account information service

Description of recipient	Purpose and legal ground
Our account information service allows you to require that the account information about and from your account is retrieved from the designated account and made available to one of our merchants or partners, as designated by you, for the purposes defined by such partner or merchant in the service which the partner or merchant provides.	<p>This means that your personal data such as transaction history and bank account number may be shared with the partners or merchants whose services you utilize and whom you have instructed us to make your data accessible to.</p> <p>The account information service may be provided to you through any of our partners or merchants that provide one or several of their own services to you and where there is a need for us to provide the services to you for the partner's or merchant's service to have the desired functionality. Please note that we are only responsible for our provision of the services to you in accordance with our own terms. The partner's or merchant's services are provided to you by the respective partner or merchant in accordance with the terms and conditions that apply for respective partner or merchant service and are thus outside the scope of this Privacy Policy. Information regarding the partner's or merchant's services is provided by the respective partner or merchant.</p>

8.1.4 Third party payment service providers

Description of recipient	Purpose and legal ground
Other third-party service payment providers that we collaborate with may be involved in connection with the provision of our services. We may share your personal data with such	We may share your personal data with a third-party payment service provider on the basis that it is necessary for us to fulfil our contractual obligations, as well as our legitimate

third-party providers when necessary for the purpose of settling the payment, preventing fraudulent use of the service and other criminal acts, and for the provider to forward the data to your merchant. If we do not share data with such third-party payment service provider when such is part of the payment chain, you will not be able to complete the transaction.	interest, to carry out the transaction and prevent fraud and other criminal acts.
---	---

8.1.5 Banks

Description of recipient	Purpose and legal ground
We may need to share your personal data and information on payments with your bank and/or other banks that are part of the payment chain.	This processing is carried out on the basis that it is necessary to fulfil our contractual obligations with you and the applicable banks.
We may need to share information on payments and your personal data to your bank and/or other banks that are part of the payment chain to investigate payment transactions, for the purposes of preventing and disclosing breaches against anti-money laundering legislation, fraudulent use of our Service and other criminal acts.	We may share your personal data with your bank and/or other banks involved in the payment chain for these purposes on the basis of our legitimate interest to prevent fraud and other criminal acts.

8.1.6 Other third parties with whom we collaborate (suppliers and sub-contractors)

Description of recipient	Purpose and legal ground
<p>We need access to services and functionalities from other companies where we cannot perform them ourselves. This means that we may need to share your data with third parties with whom we collaborate.</p> <p>For example, this means that to be able to collect personal data from a third party such as official identity verification service providers and similar service providers in order to carry out a transaction when using our service, confirm your identity, proof of funds, source of funds, as applicable, as referred to above, we will need to share some information with them.</p>	The sharing of your personal data with such third parties as listed in this section is carried out on the basis that it is necessary to fulfil our contractual obligations, our legitimate interest to carry out the transaction, our legal obligation to verify your identity and/or financial information if you use our service, and, in certain cases, your merchant's legal obligation to verify your identity.

As a rule, it is the name and/or personal identity (ID) number that are shared with them.

If you use our Service, we will also share your personal data with service providers of sanctions and PEP/RCA-lists and other similar lists in order to screen your personal data against such lists as part of our know your customer checks to assess the risk of money laundering.

We also share personal data with companies that provide cloud-based services for IT operations and the like. This is done for the purpose of providing the Service and/or to improve the Service, for example by data analysing and testing. Furthermore, we may also share your personal data to other third-party providers such as for IT-security purposes.

A third party may be a processor, which is a company that processes personal data on our behalf and in accordance with our instructions.

If and when we share your personal data with a processor, your personal data will only be processed in accordance with the purposes for which we collected your personal data in the first place. This means that a processor cannot process your personal data for additional or their own purposes.

We have a processor agreement in place with all of our processors to ensure that your personal data is protected in the same way as if we were processing your personal data ourselves and where applicable, the European Commission's standard contractual clauses (please see more information in section 10 below regarding transfers to third countries).

For a list of our processors please see here:

DevCode Identity AB, corporate registration number 559134-1960, Sveavägen 49, 113 59 Stockholm, Sweden

Roaring Apps AB - corporate registration number 559067-2613, Propellervägen 4, 183 62, Täby, Sweden

Softtronic AB - corporate registration number 559382-6502, SE- 120 32, Stockholm, Sweden

Google Cloud EMEA Limited – corporate registration number 368047, 70 Sir John Rogerson’s Quay, Dublin 2, Ireland

Zendesk Inc– 1019 Market Street, San Francisco, CA 94103

Paysolut UAB - corporate registration number 305217021, Gynėjų g. 4-333, LT-01109 Vilnius, Lithuania

UAB “Inventi” – corporate registration number 302641851, Lvivo str. 105A, Vilnius, Lithuania.

Univid AB – corporate registration number 559223-0865, Norrtullsgatan 63, 113 45 Stockholm, Sweden

8.1.7 Authorities

Description of the recipient	Purpose and legal basis
We may need to share your personal data and information on payments to governmental authorities such as the police, the Swedish Authority for Privacy Protection, financial authorities such as the Swedish Financial Supervisory Authority (Sw. <i>Finansinspektionen</i>), tax authorities and other public authorities.	<p>This is done when we are ordered to do so, when we must do so to comply with our legal obligations, or when it is necessary to investigate payment transactions for the purpose of preventing and detecting breaches of anti-money laundering legislation, fraudulent use of our services, and other criminal acts.</p> <p>When sharing your personal data for these purposes with authorities, this is carried out based on our obligation to comply with legal obligations, such as those under applicable anti money laundering and terrorist financing laws, to which we are subject or our legitimate interest in protecting ourselves from crime.</p>

8.1.8 A person holding a power of attorney for your financial affairs.

Description of the recipient	Purpose and legal basis
Your personal data may be share with a person who has been given the right to access it under a power of attorney.	We share your personal data with such holder based on our legitimate interest to handle your request provided to us via a power of attorney.

8.2 With other Brite companies

Description of the recipient	Purpose and legal basis
We may share your personal data with our group companies regardless of who you are.	This sharing is done on the basis that we have a legitimate interest in sharing data within our group for commercial, compliance and organisational reasons. The receiving Brite company will process your personal data in accordance with this Privacy Notice.

8.3 If you are a Web-site visitor

Description of the recipient	Purpose and legal basis
We may share your personal data with third party service providers of analytics tools based on your consent, for us to provide you with a pleasant user experience when interacting with our website. For more information on the cookies we use on the website, please see our cookie policy.	This sharing is done based on your consent.

9. For how long do we store your personal data?

The period for which we store your personal data varies depending on the purpose of the processing. This period may either be determined by other rules or depending on the contract we have concluded with you.

However, we always strive to minimise the period for which we store your personal data, and we never store your personal data for longer than necessary.

Please refer to the retention periods set out in section 6 above.

The legal obligations referred to above means that we cannot delete your personal data, even if you request us to delete it. If we do not have a legal obligation to retain the personal data, we instead must make an assessment if we may require the personal data in order to protect us from legal claims.

10. Where do we process your personal data?

We will always strive to process your personal data within the EU/EEA. Your personal data may be processed outside the EU/EEA in exceptional cases; for example, if a processor, either themselves or through another processor, is established outside the EU/EEA. The country we currently transfer your data to is the US. Regardless of the country in which your personal data is processed, we always take

the measures necessary to ensure that your personal data is as safe as if it were being processed within the EU/EEA.

These safeguards consist of one of the following legal mechanisms:

- ensuring that the country outside the EU/EEA is subject to an adequacy decision by the European Commission, information about which countries have been determined to have adequate protection is available on the European Commission's website https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en or https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en
- implementing and using the EU Commission's standard contractual clauses for transferring personal data which you can find here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
- ensuring that the transfer is covered by the **EU-US Data Privacy Framework**. This is an **opt-in certification system** for American companies, which is administered by the US Department of Commerce. This privacy framework encompasses a number of enforceable principles and requirements that must be certified by the American company and shall ensure that your data remains adequately protected.

More information about the EU's Standard Contractual Clauses (SCCs) for the transfer of personal data is available on the website of the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten - IMY): <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/lampliga-skyddsatgarder/>

In these cases, the recipient of personal data guarantees that the protection of your personal data under the GDPR remains applicable and that your rights are protected. If there is legislation in the receiving country that affects the level of protection for your personal data, we will implement technical and organisational security measures to maintain the protection of your personal data if it is transferred outside the EU/EEA.

If you would like to receive more information about the measures we have taken to protect your personal data if it is transferred outside the EU/EEA, please contact us at dataprotection@britepayments.com.

11. How do we use cookies?

When you are using our Services or navigate our website we may set cookies on your device. The data generated from the cookies is used to provide you with a better user experience and well-functioning experience.

We explain in more detail how we use cookies and what options you have for our cookies in our [cookie notice](#).

12. What about automated decision making and profiling?

Automated decisions with legal effect, or automated decisions that similarly significantly affect you, means that certain decisions in our services are completely automated, without our employees being involved. These decisions have a significant effect on you as an individual, comparable to legal effects. You always have the right to object to these decisions. You can read about how to object in this section.

Automated decisions that significantly affect you also mean that profiling is performed based on your data before the decision is made. This profiling is made to identify whether your use of our services involves a risk of fraud or money laundering. We profile your user behaviour and financial standing and compare this data with behaviours and conditions that indicate different risk levels for us.

When does Brite take automated decisions that significantly affect you?

We make this kind of automated decision when we:

- decide whether you pose a risk of fraud or money laundering or terrorism financing, use our services for illegal or prohibited purposes, if our processing shows that your behaviour indicates possible fraudulent conduct, or money laundering, that your behaviour is not consistent with previous use of our services, or that you have attempted to conceal your true identity. We also screen you against sanction lists and lists of PEP/RCA in accordance with anti-money laundering legislation to fulfil our legal obligations.

If you are not approved under the automated decisions described above, you will not have access to our services. The outcome of the automated decision may also be change of risk classification, blocking, hold or release of transactions.

We have several safety mechanisms to ensure the decisions are appropriate. These mechanisms include ongoing overviews of our decision models and random sampling in individual cases.

You can always contact us, if you have any concern about the outcome, and we will determine whether the procedure was performed appropriately. You can also object in accordance with the following instructions.

The processing of your personal data in this automated decision making is carried out on the basis that it is necessary for us to fulfil our contractual obligations towards you to carry out payments or to comply with legal requirements, particularly those related to our obligations to conduct know your customer checks in relation to our anti-money laundering obligations, as the case may be.

Your right to object to these automated decisions

You always have the right to object to an automated decision with legal consequences or decisions which can otherwise significantly affect you (together with the relevant profiling) by sending an



e-mail message to dataprotection@britepayments.com . A Brite employee will then review the decision, taking into account any additional information and circumstances that you provide to us.

13. Do you have a complaint relating to our processing of personal data?

Please contact dataprotection@britepayments.com if you wish to file a complaint relating to our processing of your personal data. You can also file a complaint with the Swedish Authority for Privacy Protection. The Swedish Authority for Privacy Protection is the Swedish national supervisory authority as regards the processing of personal data according to, for example, GDPR. Visit <https://www.imy.se/> in order to file a complaint with the Swedish Authority for Privacy Protection. You can also file a complaint with the data protection authority in your homeland within the EU.

14. Amendments to this Privacy Notice

We are entitled to amend this Privacy Notice when required. When we make amendments that are not purely linguistic or editorial, and the changes affect personal data previously collected, you will receive clear information about the amendments and what they entail for you before they start to apply.

Amendments will not apply for you if we need your consent to implement the amendments and you do not accept them.
