

TRUSTLY'S PRIVACY POLICY

Published on 2024-05-08

1. Who are we?

Trustly Group AB, reg. no. 556754-8655 ("Trustly", "we", "us" or "our") is a Swedish payment institution providing online banking payment solutions across Europe. We are licensed by the Swedish Financial Supervisory Authority to conduct our activities, and are responsible as data controller for the processing of your personal data under this privacy policy.

2. Why this privacy policy?

At Trustly, we value your privacy and we work hard to make sure that we process your personal data in accordance with the requirements set out in the General Data Protection Regulation (EU) 2016/679 (the "GDPR") and other applicable data protection legislation.

You can interact with us in several ways. In this privacy policy, we provide you with information on how we process your personal data if you are an/a:

End-user that is using our payment service(s);

Customer representative that is representing a current or potential customer of ours (including owners of such, ultimate beneficial owners and legal representatives); and/or

Website visitor that is interacting with our websites or contacting our support and/or complaints services.

If you apply for a job with us, please read our privacy policy for job applicants which you can find in connection with submitting your application.

If we process your personal data for other purposes than those described in this privacy policy we will provide you with a separate privacy notice informing you about such processing.

3. What personal data do we process about you?

Depending on how you interact with us and for what purpose, we collect and process different types of personal data about you. In order for you to more easily understand what type of personal data we may process about you, we have categorised the personal data into the following categories, including data elements:

Identifying Information – first name, last name, home address (including e.g. flat/house number), telephone number, email address, date of birth, nationality, citizenship, personal identity number, passport number, and/or identity card number, and End-user ID. This information is usually provided to us directly by you as an End-user or a Customer representative. The information can also be collected from your online

banking interface (i.e. online bank) or via an API provided by your bank, and/or be provided from your Merchant and/or external third party sources.

Order Identifying Information – information identifying an End-user’s payment, such as order id number, message id, notification id and the time when the transaction was made. This information is usually provided by your Merchant. The information may also be generated by our payment system.

Financial Information – sending and/or receiving bank, bank account ownership, bank account number, account balance at the time of the payment, source of funds and proof of funds. This information is usually provided by your bank or directly by you.

Device Information – IP-address, type of device, operating system and browser information. This information is usually collected by us using cookies or similar technology.

Behaviour Information – how End-users use our payment service and/or how Website visitors interact with our websites. This information is usually collected by us using cookies or similar technology.

Information related to your contacts with Trustly’s customer service – information provided by you through channels available on our websites, such as contact forms, payment lookup tool, chat conversations and email correspondence.

Sensitive Information – Depending on what information you may provide Trustly with in relation to the purposes for processing, as stated in Section 4 below, Trustly may collect sensitive personal information as defined in Article 9 in the GDPR. Trustly may also process such sensitive information in relation to e.g. the purpose of screening your personal information against lists of politically exposed persons (“PEP”) and lists of persons subject to sanctions. Such sensitive information may include personal data that reveals racial or ethnic origin, religious beliefs, political or philosophical views, trade union membership, or information about health or sexual orientation.

4. For what purpose do we process your personal data and what legal basis do we rely on?

We use and share the personal data we collect about you for several different purposes and we rely on different legal bases. Depending on if you are an End-user using our Service (as defined below), a representative to a current or potential customer of ours or a Website visitor interacting with our website, the below tables sets out which categories of personal data we process, for what purpose and the legal ground we rely on when doing this. Further down in this privacy policy, we will also describe how we collect your personal data, and whom we may share it with, as well as the legal basis that allows us to do this.

4.1. When you as an End-user use our Service

Providing our Service

Trustly’s proprietary, bank independent, online payment solution enables initiation of account-to- account bank transfers online (the/our “Service”). The Service consists of several different features which allows you to:

(a) initiate payments from your online bank in a fast, simple and secure manner to an online supplier providing you with a product or service (the “Merchant”), meaning that you can pay for goods and services directly from your bank account (“Pay-in”);

(b) receive payments from the Merchant directly to your bank account in case you e.g. want to return purchased goods (“Pay-out”);

(c) verifying your bank account to register a direct debit mandate that will allow us, or your Merchant, to initiate payments directly from your bank account (“Direct Debit Payment”) without the need for you to login to your bank for each purchase;

(d) authenticate yourself towards a Merchant and/or register an account with the Merchant when making a payment transaction where the Merchant has such identification requirements (“Identity Verification”); and/or

(e) verifying your bank account towards a Merchant (“Account Verification”).

Below we will describe how we process your personal data when using the different features of the Service.

Purpose of the processing	Legal basis	Personal data processed
To initiate and process a convenient and secure Pay-in to your Merchant.	Contractual obligation.	Identifying Information, Order Identifying Information, Financial Information, Device Information.
To initiate and process a convenient and secure Pay-out to you from your Merchant.	Contractual obligation.	Identifying Information, Order Identifying Information, Financial Information, Device Information.
To set up a direct debit mandate in a convenient way and to conduct a Direct Debit Payment.	Contractual obligation.	Identifying Information, Order Identifying Information, Financial Information, Device Information.
To verify your identity and/or update your contact information when the Service is used for Identity Verification, i.e. as a means for you to verify your identity towards your Merchant.	Contractual obligation.	Identifying Information.

To refresh your Identifying Information in case of Identity Verification (will be made on a 180-day interval).	Pursue our legitimate interest in providing you with the Service.	Identifying Information.
To verify your bank account when the Service is used for Account Verification.	Contractual obligation.	Identifying Information, Financial Information.

Comply with legal and regulatory obligations

As a licensed payment institution, Trustly is obliged to follow a set of laws and regulations relating to its processing of payment transactions. Some of the data we collect about you when you use our Service will be used to fulfil these legal and regulatory obligations.

For more detailed information on what data we use for legal and regulatory compliance purposes, see the table below.

Purpose of the processing	Legal basis	Personal data processed
To fulfil our legal obligations to conduct know your customer checks on you (including performing enhanced due diligence when applicable), which includes verify your identity, e.g. through sending you a letter or contact you via email, and assess your financial information, screening your personal information against lists of politically exposed persons (“PEP”) and lists of persons subject to sanctions and other similar lists to assess if you imply a money laundering risk. This processing constitutes profiling and automated decision-making. More information about profiling and automated decisions can be found in section 8.	Comply with legal obligations. To the extent the information constitutes Sensitive Information, the legal basis is that the processing is necessary for reasons of public interest (Article 9(2)(g) GDPR). The Sensitive Information may contain e.g. information about political opinion and/or religious beliefs contained in PEP lists and health information contained in proof/source of funds.	Identifying Information, Financial Information, Device Information, Sensitive Information.
To fulfil our legal obligations under applicable money-laundering regulations to monitor	Comply with legal obligations. To the extent the information constitutes Sensitive	Identifying Information, Order Identifying Information, Financial

the payments processed by us and to report suspicious payments to the police or similar authorities. This processing constitutes profiling and automated decision-making. More information about profiling and automated decisions can be found in section 8.	Information, the legal basis is that the processing is necessary for reasons of public interest (Article 9(2)(g) GDPR). The Sensitive Information may contain e.g. information about political opinion and/or religious beliefs contained in PEP lists.	Information, Device Information, Sensitive Information.
To fulfil our legal obligations to report statistics to authorities on <i>inter alia</i> fraudulent transactions.	Comply with legal obligations.	Identifying Information, Order Identifying Information, Financial Information, Device Information.
To fulfil our legal obligations to contact you if a situation would arise that may affect your financial interests or, if you use our Direct Debit Payment service, to inform you about changes to our terms for use of this service.	Comply with legal obligations.	Identifying Information.
To fulfil our legal obligations under bookkeeping law pursuant to which we are obliged to store your personal data relating to a payment.	Comply with legal obligations.	Identifying Information, Order Identifying Information, Financial Information.

Performance and business development

At Trustly, we always strive to provide you with the best possible user experience. In order to achieve this, we will process your personal data to make sure that our Service works properly and to fix any problems that may occur in the Service. We also use your personal data to ensure that the Service is presented to you in the best way and to understand how we can develop our Service to create even better products.

For more detailed information on what data we use for these performance and business development purposes, see the table below.

Purpose of the processing	Legal basis	Personal data processed

To troubleshoot the Service in case of lack of performance.	Pursue our legitimate interest in troubleshooting the Service in order to provide you with a working Service.	Identifying Information, Order Identifying Information, Financial Information, Device Information, Behaviour Information.
To perform analysis on how you use our Service, to develop our Service and to test the functionality of our Service.	Pursue our legitimate interest in developing our Service in order for us to continue offering the best possible products and services to you.	Identifying Information, Order Identifying Information, Financial Information, Device Information, Behaviour Information.
To adapt the presentation of the interface, such as the type of language and appearance of our Service, through which we communicate with you, depending on what type of device you use.	Pursue our legitimate interest in adapting the presentation of the Service to you.	Device Information and Identifying Information.
To perform data analysis for product development and testing in order to improve our processes for fulfilling legal obligations, such as conduct know your customer checks and prevent fraud, and to design our Service (if possible, we first anonymise the data, which means that no personal data processing is performed thereafter).	Pursue our legitimate interest in performing data analysis for product development and testing.	Identifying Information, Order Identifying Information, Financial Information, Device Information.

Incident management and security

To manage incidents and mitigate the risk that the Service is being used for fraudulent and other illicit actions, we may process your personal data for these types of purposes.

For more detailed information on what data we use for this incident management and security purpose, see the table below.

Purpose of the processing	Legal basis	Personal data processed

<p>To prevent our Service from being used for frauds and/or similar illicit actions. This processing constitutes profiling and automated decision-making. More information about profiling and automated decisions can be found in section 8.</p>	<p>Comply with legal obligations to prevent and detect crime such as frauds.</p> <p>To the extent the information constitutes Sensitive Information, the legal basis is that the processing is necessary for reasons of public interest (Article 9(2)(g) GDPR). The Sensitive Information may contain e.g. information about political opinion and/or religious beliefs contained in documentation submitted by you.</p>	<p>Identifying Information, Order Identifying Information, Financial Information, Device Information, Sensitive Information.</p>
<p>To ensure that you reside in a country where we offer our Service. This processing constitutes profiling and automated decision-making. More information about profiling and automated decisions can be found in section 8.</p>	<p>Contractual obligation.</p> <p>To the extent the information constitutes Sensitive Information, the legal basis is that the processing is necessary for reasons of public interest (Article 9(2)(g) GDPR). The Sensitive Information may contain e.g. information about political opinion and/or religious beliefs contained in documentation submitted by you, e.g. for the purpose of verifying your country of residence.</p>	<p>Identifying Information, Device Information, Sensitive Information.</p>
<p>To ensure a high level of IT-security in order to keep your personal data safe, by e.g. preventing the Service from being targeted by cyber-attacks.</p>	<p>Pursue our legitimate interest of keeping your personal data safe as well as ensuring that our Service is working as intended in case of a cyber-attack.</p>	<p>Identifying Information, Order Identifying Information, Financial Information, Device Information.</p>
<p>To fulfil our contractual obligations to inform our Merchant of incidents.</p>	<p>Pursue our legitimate interest of informing our Merchants of incidents.</p>	<p>Identifying Information, Order Identifying Information, Financial Information, Device Information.</p>
<p>To fulfil our legal obligations to</p>	<p>Comply with legal obligations.</p>	<p>Identifying Information,</p>

report certain incidents to the Swedish Financial Supervisory Authority and the Swedish Authority for Privacy Protection.		Order Identifying Information, Financial Information, Device Information.
To establish, exercise and/or defend Trustly against legal claims.	Pursue our legitimate interest of establishing, exercising and/or defending legal claims.	Identifying Information, Order Identifying Information, Financial Information, Device Information.

“Remember me” functionalities

When you are using our Service, we may set cookies on your device to remember your information for the next time you use our Service. The data generated from the cookies is used to provide you with a better user experience. For more information on how Trustly uses cookies, see section 4.4 below.

For detailed information about how we use the data generated from the cookies we place when you use our “remember me”-functionalities, see the table below.

Purpose of the processing	Legal basis	Personal data processed
To enable a convenient payment experience, Trustly uses a so-called “remember me” functionality which allows us to remember and autofill your telephone number for your coming visits. Please see more information about this functionality below (“Remember me” functionalities).	Your consent. If you want to withdraw your consent and thus disable the functionality, you can choose such an alternative by checking a box which will be shown on your next visit/use of the Service. Alternatively, you can read our cookie policy available here for more information on how you can remove cookies.	Identifying Information, Device Information, Behaviour Information.
To enable a convenient payment experience, Trustly uses a so-called “remember me” functionality which allows us to remember your bank and account number or user-ID in order to autofill your account number for coming visits. Please see more information about this functionality below (“Remember me” functionalities).	Your consent. If you want to withdraw your consent and thus disable the functionality, this can be done easily by opting out (which you do by using the toggle shown next to your bank account on your next visit/use of the Service). Alternatively, you can contact our Support function here and they can assist you.	Identifying Information, Device Information, Financial Information, Behaviour Information.

“Remember me” functionalities

When you use our Service, you may choose to activate/opt in to our functionality which remembers your telephone number, bank and account number or your user-ID that you use to log in to your online bank, for instance a personal ID-number or a username (please note that we will never store any passwords you use to log in to the online bank) for the purpose of providing you with a convenient payment experience the next time you choose to pay with Trustly for goods or a service provided to you by a Merchant. We will remember you regardless which Merchant you are initiating the payment to/from.

These functionalities enable us to, the next time you use Trustly, save you the trouble of entering your telephone number, choosing your bank, login method and preferred bank account. To achieve this we will, the next time you use our Service, prefill your telephone number, your user-ID or the account number to the bank account you have asked us to save.

The functionality will be activated from when you have switched it on, until you decide to switch it off. If you choose to switch off this functionality, and thus withdraw your consent, we will disable the functionality and no longer process your remembered information for the purpose of providing you with a smooth and convenient payment experience. The next time you pay with Trustly, you will then have to type in your telephone number again. You may also have to verify your telephone number an additional time in order for us to present you with our Service. For your user-ID or bank and account number, as applicable, you will then have to fill in your userID, or as applicable, choose your bank, your login method and preferred account. You will also have to verify your identity an additional time in order for us to present your available bank accounts to you from which you can make a payment.

When choosing to activate one or both of the above functionalities, we will place a cookie/cookies on your device. We will assign this cookie/these cookies a randomised value which our software will recognise when you return. The randomised value does not in itself contain any personal information but is only a means for us to know that you have agreed to the faster payment functionality and will trigger our software to optimise your payment flow.

Functionalities for a faster Service

For detailed information about how we process your data for the purpose of providing a faster service, see the table below.

Purpose of the processing	Legal basis	Personal data processed
Trustly collects your details in connection with your use of the		

<p>Service to later use this information for the purpose of recognizing your details from previous visits to offer you a faster payment experience. Please see more information about this functionality below (Faster payment experience for Pay-ins).</p>	<p>Pursue our legitimate interest in offering you a faster payment experience.</p>	<p>Device Information, Financial Information, Identifying Information.</p>
<p>To create a fast and convenient payment experience when you perform Pay-ins, we will store your opt in/consent for us to remember your preferred bank account. Please see more information about this functionality below (Faster payment experience for Pay-ins).</p>	<p>Your consent. If you want to withdraw your consent and thus disable the functionality, this can be done easily by opting out (which you do by using the toggle shown next to your bank account on your next visit/use of the Service).</p>	<p>Behaviour Information, Device Information, Financial Information.</p>
<p>To create a fast and convenient payment experience, we will as applicable, prefill your “country” as part of performing our know-your-customer checks.</p>	<p>Pursue our legitimate interest in providing you with a faster payment experience.</p>	<p>Device Information, Financial Information.</p>
<p>To create a fast and convenient payment experience when you perform Pay-outs, we will, as applicable, display the bank account that you used for your last transaction with Trustly.</p>	<p>Pursue our legitimate interest in providing you with a faster payment experience.</p>	<p>Financial Information, Identifying Information.</p>
<p>To create a fast and convenient payment experience when you perform recurring Pay-ins with a specific Merchant, we will enable the Merchant to display the bank account that you used for your last Trustly transaction made with that specific Merchant. Please see more information about this functionality below</p>	<p>Pursue our legitimate interest in providing you with a faster payment experience.</p>	<p>Identifying Information.</p>

(Faster payment experience for Merchant specific Pay-outs).		
---	--	--

Faster payment experience for Pay-ins

To provide you with a faster payment experience, we will collect and use Identifying Information provided from your Merchant and your Device Information to recognize you when you use our Service, regardless which Merchant you are initiating the payment to. This enables us to ask whether you wish for us to display your latest used bank account in the payment flow which gives you the opportunity to leverage a faster payment experience on a returning basis.

Further, when you have opted in for us to remember your preferred bank account for a faster payment experience, we will store your consent to recognize you the next time you choose to pay with Trustly for goods or a service provided to you by a Merchant, i.e. we will remember you regardless which Merchant you are initiating the payment to and regardless of which device you use. This will make it possible for us to provide a faster payment experience (showing your last used bank account and enabling you to skip the login step to your bank). If you wish to withdraw your consent, this can be done easily by opting out, which you do by using the toggle shown next to your bank account on your next visit/use of the Service, or by contacting our customer support.

In addition to the above and when logged in to your bank, you will also, when you activate our faster payment functionality, give us your consent to communicate to your bank that you for a period of 180 days (as applicable from bank to bank), allow us to fetch and display your account for a faster payment. We will only use this access when you have initiated a payment with Trustly to make your requested payment.

Faster payment experience for Pay-outs

As applicable, to provide you with a faster experience when you initiate a Pay-out, we will, for each bank you sign into, save the bank account that you use for your transaction with Trustly. This enables a faster Pay-out experience the next time you use Trustly as we will display your bank account without you having to sign in to the bank.

Faster payment experience for Merchant specific Pay-ins

In order for us to provide you with a faster payment experience with a specific Merchant, Trustly will, when you make your first transaction with a specific Merchant, create a unique identifier that Trustly will share with the Merchant. The next time you return to the Merchant's checkout and want to perform a transaction using Trustly, the unique identifier will in turn be sent to Trustly by the Merchant in order to recognise you. This enables your Merchant to display your latest used bank account in the payment flow, which gives you the opportunity to leverage a faster payment experience on a returning basis.

How do we collect your personal data when using the Service?

When using our Service, we collect your personal data directly from you, as well as from your online banking interface (i.e. online bank) or via an API provided by your bank. In addition, we also collect personal data from your Merchant and from external third-party sources. For example, the latter can occur as part of our know your customer checks, for instance when we need to verify your identity, proof of funds, source of funds and/or update/supplement contact information via official identity verification service providers or

similar providers, as applicable. Our payment system will in addition generate personal data such as an order id number when you use our Service.

Trustly also resells payment services provided by third party payment service providers. When reselling such payment services, Trustly will obtain personal data about you from such providers. For more information about which personal data a third-party payment service provider shares with Trustly, please contact the relevant provider.

4.2. When you are a Customer representative

Trustly process personal data of representatives for our customers being the Merchants or another payment service provider that resells our Service via their channels. This processing is mainly done to administer the business relationship and fulfil our legal obligations to conduct so-called know your customer checks on our customers. If you as a Customer representative provide information regarding other people in your organisation or outside of your organisation, you are responsible for informing them that their data will be processed in accordance with this Privacy Policy.

In this section, you can find more specific information on how we process your data in case you are a Customer representative.

Purpose of the processing	Legal basis	Personal data processed
<p>To fulfil our legal obligations to conduct know your customer checks on you as Customer representative (including performing enhanced due diligence when applicable), which includes verifying your identity and screening of your personal information against PEP-lists and lists of persons subject to sanctions and other similar lists to assess if you imply a money laundering risk. This processing constitutes profiling and automated decision-making. More information about profiling and automated decisions can be found in section 8.</p>	<p>Comply with legal obligations.</p> <p>To the extent the information constitutes Sensitive Information, the legal basis is that the processing is necessary for reasons of public interest (Article 9(2)(g) GDPR). The Sensitive Information may contain e.g. information about political opinion and/or religious beliefs contained in PEP lists.</p>	<p>Identifying Information and when applicable copies of your passport and other documents validating your identity and/or address and Sensitive Information.</p>
<p>To enter into, manage and maintain a business relationship with you and the company you represent and to communicate important information regarding</p>	<p>Pursue our legitimate interest in communicating, managing and maintaining contact with you and the company you represent as well as to verify that the</p>	<p>Identifying Information.</p>

our Service that is not considered marketing.	information we have about you is up to date or if we need to communicate information to you about our Service that we assess is important for you to be aware of.	
To improve our Service, we may send out customer satisfaction surveys to you. In such surveys, we will ask you to <i>inter alia</i> evaluate us and/or our Service.	Pursue our legitimate interest in improving our Service in order to be able to provide a better Service or develop new services based on the answers to the survey.	Identifying Information.
To market our Service e.g. in case you show interest in our Service by e.g. visiting our events and/or websites (see more under section 4.3 for more information), or if we have reason to believe that you as a Customer representative would be interested in our Service. There is always an opportunity to opt-out from marketing in an easy and convenient way, e.g. by clicking “unsubscribe” to the emails we or our advertising agencies might send or by objecting to the processing of your personal data for this specific purpose.	Pursue our legitimate interest of marketing our Service for commercial purposes and to offer our Service or new services that we think you as a Customer representative would be interested in.	Identifying Information, Behaviour Information.

How do we collect your personal data when you are a Customer representative?

When you contact us for the purpose of entering into a potential business relationship regarding our Service, we will collect the personal data that you provide us with, such as contact details from emails and agreements. We will also collect personal data provided by you if you, for example, give us your contact details in relation to campaigns you want to take part of or white papers you wish to receive. Additionally, we may collect your contact details in your capacity as a potential Customer representative from third-party suppliers of Customer registers, or publically available sources such as company websites, for the purpose of marketing our Service to you, if we believe that you would be interested in our Service.

When conducting know your customer checks on you as a Customer representative, we will ask you to provide information, such as passport copies on e.g. its ultimate beneficial owners and directors.

In addition to the information that we receive from you, we will also collect personal data about you through cookies if you visit our websites (see more under section 4.4 for more information).

4.3. When you contact our support and/or complaints service

We value your feedback and we want to understand what we can do to improve our Service and answer any questions that you may have. Therefore, Trustly has a customer support platform available where you can get in contact with us. When you do this, we will collect certain personal data about you.

In this section, you can find more specific information on how we process your data in case you are an individual contacting our support and/or complaints service or if you are a Website visitor.

Purpose of the processing	Legal basis	Personal data processed
To assist you with your question or concern in case you contact our support and/or complaints service, either through channels available on our websites, such as contact forms, transaction lookup tool or chat function, or by emailing us.	To fulfil our Contractual and Legal obligation to provide you with a complaints service.	Identifying Information, Order Identifying Information, Device Information, Financial Information, Information related to your contacts with Trustly's customer service.

How do we collect your personal data when you contact our support and/or complaint service or visit our websites?

If you contact us, we will process your personal data by collecting your contact details through the media you choose to contact us, i.e. via email, post, social media or any other way. Similarly, when visiting our websites, we will process your personal data by setting cookies on your device and thus collect information in accordance with our cookie policy.

4.4. Our use of cookies

Trustly uses cookies on our websites and checkout in order to deliver a well-functioning, personalized and user-friendly experience. Please read our cookie policy for our use of cookies on our website, available [here](#), and our use of cookies in our checkout, available [here](#).

4.5. Other situations

Regardless of who you are, personal data about you may also be processed by us for the purpose of fulfilling your rights as a data subject under the GDPR and to establish, exercise and defend ourselves against legal claims. For more information, please see below.

Purpose of the processing	Legal basis	Personal data processed
To cater to your rights in accordance with the GDPR and other applicable data protection legislation. For example, if you, as a data subject, contact us and ask us to provide you with the information we have collected about you, we will ask you to verify yourself in order to prevent disclosure of personal data to the wrong person.	Comply with legal obligations and pursue our legitimate interest of verifying your identity in order to prevent disclosure of personal data to the wrong person.	Identifying Information, Order Identifying Information, Financial Information, Device Information.
To handle any complaints or establish, exercise and/or defend Trustly against legal claims.	Pursue our legitimate interest of handling complaints or establish, exercise and/or defend legal claims.	Identifying Information, Order Identifying Information, Financial Information, Device Information.

Social Media

We use social media networks such as Facebook, Twitter and Instagram in our marketing activities. The providers of these networks collect and process personal data from you as a user of the platform. We do not collect personal data from users who visit our social media accounts without specifically informing you or, when legally required, collecting your consent in each specific case, such as in the case of a competition. In such cases the personal data that we would collect would consist of your user-id/username from the relevant social media network. This personal data is processed in order for us to fulfil our contractual obligations with you or, as applicable, on the basis of your consent. Such personal data will only be kept until the winner of the competition has been disclosed and the competition has been finalized.

5. With whom do we share your personal data?

The information 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 End-users, Customer representatives and Website visitors and other individuals contacting our support and/or complaint service.

When Trustly shares your personal data with third parties, this is done in a responsible way and in accordance with applicable data protection legislation.

5.1. General

Trustly Group

Regardless of who you are, your personal data may be shared with companies that form part of the Trustly Group, when needed to fulfil the purpose the data was collected for. This sharing of data is carried out on the basis that we have a legitimate interest in sharing data within our group for commercial, compliance and organisational reasons.

The group company that we share your personal data with can act as (i) data processor, meaning that it will process your personal data on our behalf and in accordance with our instructions, (ii) independent data controller, meaning that the group company processes your personal data for its own and independent purposes, and as such is solely responsible for the processing or (iii) joint controller, meaning that Trustly and the group company jointly decide both the purpose and the means of the processing, and as such are jointly responsible for the processing.

Joint controllership

In case of joint controllership, we, together with the relevant group company, are obliged under the GDPR to determine and allocate our respective responsibilities for compliance with the obligations under the GDPR. We are also obliged to make the essence of this arrangement available to you. Please see below for such information.

Direct Debit Payment

If you are using our Direct Debit Payment service within the Eurozone area, we will share your personal data with our group company SlimPay, for the purpose of providing the service. When providing this service, Trustly and SlimPay act as joint controllers in relation to the processing of your personal data.

Trustly is responsible under the GDPR to provide you with information on how your personal data is processed for the purpose of the Direct Debit Payment service. Trustly is also the primary recipient of requests related to your rights under the GDPR (see section 9 below), such as your right to get access to what personal data we and/or SlimPay process about you. However, you are free to exercise your rights towards SlimPay if you wish.

You can find more information on how SlimPay processes your personal data, such as the legal basis that SlimPay relies on and the ways to exercise data subject rights against SlimPay, [here](#).

5.2. When you as an End-user use our Service

Your Merchant

For the purpose of 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. What type of information we send to

your Merchant depends on the type of transaction and how the Merchant integrates the Service in their system.

Identifying Information and/or Financial Information may also be forwarded to your Merchant in order for the Merchant to verify your identity when the Service is used for Identity Verification and/or Account Verification. We share this information with the Merchant if the Merchant is legally obliged to verify your identity as a measure to prevent money laundering, or otherwise needs this data to prevent fraud, or other criminal acts or to meet other potential legal and/or regulatory requirements imposed on the Merchant. In certain situations, 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. Your personal data may also be shared with Merchants in order for them to provide a faster payment experience in their checkout. In these cases, if you are logged in to the Merchant's website, the Merchant may automatically fill in a few digits of your bank account as well as your bank when you reach their checkout. Such autofilling is handled by the Merchant and if you do not want your details to be automatically filled in, you need to log out of the Merchant's website before visiting their checkout.

The sharing of your personal data with the Merchant 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. In addition, our legitimate interest in sharing your personal data with your Merchant is sometimes based on your wish to share your personal information to your Merchant in order for you to verify your identity, bank account and/or use your Merchant's service, which we provide a simple and convenient solution for.

If one of our contracted Merchants merge, 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 above, with the acquiring Merchant which takes over the contract with us as part of such merge, acquisition or restructure. This sharing 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.

Third party payment service providers

When offering our Services, other third-party payment service providers that we collaborate with may be involved. In such case, we will share your personal data with such third-party providers when necessary for the purpose of settling the payment, preventing fraudulent use of the Service and other criminal acts, and in order for the provider to forward the data to your Merchant. If we do not share data with such third-party payment service providers when such is part of the payment chain, you will not be able to complete the transaction.

This sharing of your personal data with a third-party payment service provider 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.

For more information about which personal data a third-party payment service provider shares with Trustly, please contact the relevant provider.

Authorities, banks and payment schemes

To carry out a transaction when using our Service, we need to transfer some of your personal data to your bank and other banks that are part of the payment chain, and relevant national payment schemes such as

BACS in the United Kingdom and Bankgirot in Sweden. This processing is carried out on the basis that it is necessary to fulfil our contractual obligations. We may also need to transfer your personal data to relevant national payment schemes for the purpose of troubleshooting payments. This processing is carried out on the basis of our legitimate interest.

We may also need to share your personal data and information on payments to police, tax and other relevant authorities, and possibly your bank and/or other banks that are part of the payment chain. This is done when necessary to investigate payment transactions for the purposes of preventing and disclosing breaches against anti-money laundering legislation, fraudulent use of the Service and other criminal acts. We may also share your personal data with authorities for audit purposes. When sharing your personal data for these purposes with authorities, this is carried out on the basis of our obligation to comply with legal obligations to which we are subject. When sharing your personal data for these purposes with your bank and/or other banks that are part of the payment chain, this is carried out on the basis of our legitimate interest to prevent frauds and other criminal acts.

Further, we may need to share your personal data with banks in order for them to fulfil their obligation to perform know your customer-procedures on us (upon onboarding or as otherwise necessary during our partnership with such bank). When sharing your personal data for these purposes with your bank and/or other banks that we use, this is carried out on the basis of our legitimate interest to prevent frauds and other criminal acts.

Other third parties with whom we collaborate

To carry out a transaction when using our Service, we may need to share your personal data with collaboration partners such as official identity verification service providers and similar service providers in order to confirm your identity, proof of funds, source of funds and/or update/supplement your contact information, as applicable. To be able to use such identity verification service providers we may need to share your personal data for the purpose of verifying the functionality of the service provided. The sharing of personal data with such third parties is carried out on the basis that it is necessary to fulfil our contractual obligations, our legal obligation to verify your identity and/or financial information if you use our Service, and, sometimes, your Merchant's legal obligation to verify your identity.

If you use our Service, we will also share your personal data with service providers of sanctions and PEP-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 if you imply a money laundering risk. The sharing of personal data is then carried out on the basis that it is necessary in order to comply with our legal obligations.

In addition, we will share your personal data with cloud-based service providers, such as providers of technical server capacity. This is done for storage and 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.

When your personal data is shared with such third parties, the third party will typically act as data processor in relation to your personal data, meaning that it will process your personal data on our behalf and in accordance with our instructions.

5.3. When you are a Customer representative

Trustly Group

If a Merchant of Trustly is to become a customer of another company that forms part of the Trustly Group, Trustly may share your personal data related to CDD/EDD with such company for such company's own KYC purposes. The receiving group company will then be responsible (independent data controller) for the processing of this personal data. For further information on such group company's processing, please see relevant group companies' privacy policies here:

[SlimPay](#)

Trustly UK

Ecospend Technologies

Providers of sanctions and PEP lists and other similar lists

If you are a Customer representative, we may need to share your personal data with providers of sanctions and PEP 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 implications of any money laundering risks. The sharing of personal data is then carried out on the basis that it is necessary in order to comply with our legal obligations.

Authorities and banks

We may need to share your personal data to the police, tax and other relevant authorities, and possibly banks that are part of the payment chain (of our End-users). This is done when necessary to investigate payment transactions for the purposes of preventing and disclosing breaches against anti-money laundering legislation, fraudulent use of the Service and other criminal acts. We may also share your personal data with authorities for audit purposes. When sharing your personal data for these purposes with authorities, this is carried out on the basis of our obligation to comply with legal obligations to which we are subject. When sharing your personal data for these purposes with your bank and/or other banks that are part of the Merchant's/End-user's payment chain, this is carried out on the basis of our legitimate interest to prevent frauds and other criminal acts.

Other third parties with whom we collaborate

In addition, we will share your personal data with cloud-based service providers, such as providers of technical server capacity or CRM providers. 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. When sharing your personal data for these purposes with said third parties, this is carried out on the basis of our legitimate interest to provide and/or to improve the Service and maintain a high level of IT-security.

Furthermore, we may also share your data to third-party providers such as external advertising agencies. We share this information on the basis that we have a legitimate interest of marketing, through professional advertising agencies, to you regarding products and services that you have shown an interest in.

When your personal data is shared with such third parties, the third party will typically act as data processor in relation to your personal data, meaning that it will process your personal data on our behalf and in accordance with our instructions.

5.4. When you visit our websites, contact our support and/or complaints service

We may share your personal data to other third-party providers of analytical tools based on your consent, in order for us to provide you with a pleasant user experience when interacting with our websites.

If you are a Customer representative, we may also share your personal data with third party payment providers for the purpose of providing you with an opportunity to be onboarded by such payment providers. We will only share your personal data for this purpose based on your consent.

In addition, we may from time to time also need to share your personal data with cloud-based service providers, such as providers of technical server capacity.

5.5. When you use our-/interact with us on social media

If you interact (e.g. like/comment a post, contact or follow us) with our designated accounts on social media such as Facebook, Instagram or Twitter, your personal data will also be collected and processed by these companies, in accordance with their data protection information. This also applies to the response you receive from us. The sharing takes place to pursue our legitimate interest of interacting with you in case of e.g. questions or complaints on our social media.

5.6. Persons holding a power of attorney for an End-user

Your personal data may be shared with a person who has been given the right to access it under a power of attorney. Trustly shares your personal data with such holder based on our legitimate interest to handle your request provided to us via a power of attorney.

5.7. Mergers and acquisitions

We may need to share your personal data and information in connection with planned and/or finalized company acquisitions or restructuring of the Trustly Group. If Trustly is to be restructured, e.g. is divided into several different operations, or if an outside party wishes to acquire Trustly, we will disclose your and other customers' personal data to the acquiring company. This may entail any personal data which you have provided to us or that we have collected in connection with our Services. This processing is carried out on the basis of our legitimate interest in enabling an acquisition or restructuring process. If Trustly ceases to exist, e.g. through a merger, liquidation or bankruptcy, we will transfer or delete your personal data as long as we do not need to save them to meet legal requirements. If Trustly is acquired by an acquiring company or split up in connection with a restructuring, we will continue to save and use your personal data according to the terms herein, unless you receive other information in connection with the transfer/such acquisition.

6. For how long do we process your personal data?

We will process your personal data for as long as we need to fulfil the purpose(s) the data was collected for.

Personal data processed to fulfil our contractual obligations towards you when you use our Service are stored during the contractual relationship and thereafter during a period of at a minimum 7 years from the payment to fulfil bookkeeping law. Generally, this time period is extended to 10 years based on statutes of limitations, for the purpose of establishing, exercising and/or defending Trustly against legal claims. To fulfil anti-money laundering law, we may need to store your data for additional 5 years after we have ceased to provide the Service to you or your Merchant, unless anti-money laundering law requires us to store your data longer.

Personal data about Customer representatives will, as a main rule, not be stored for a longer period than five (5) years from the end of the business relationship between Trustly and the Merchant, unless we are required by law to store your data longer.

Personal data that is processed for other purposes than for the performance of your contract with Trustly or for Trustly to fulfil legal obligations are processed as long as necessary to fulfil the respective purpose the personal data was collected for.

Please note however that during the time we store your personal data, the data will not be processed for all of the purposes set out above in this privacy policy. Different time periods for processing of your personal data apply depending on the purpose the data was collected for. For example, one set of data, e.g. Financial Information, will be processed for several purposes and may for some purposes be processed only for a very short period of time but for other purposes for longer periods of time. Trustly has implemented various technical and organisation measures, such as automated deletion of data and access restriction to systems where personal data is stored, to ensure that the data is not used for a longer period than necessary to fulfil the respective purpose the data was collected for.

7. Where and how do we store your personal data?

We typically store your personal data on servers located within the EU/EEA. However, sometimes, your Merchant and/or other third parties that we share your data to, are located outside the EU/EEA. This also applies in case we share your personal data with our UK and US companies that form part of the Trustly Group. If your personal data would be transferred to, and processed by, a Merchant, within the Trustly Group, or a third party in a country outside the EU/EEA, we will take all reasonable measures to ensure that your data is processed with a high level of security with an adequate level of protection maintained, and that suitable safeguards are adopted in line with applicable data protection legislation requirements, such as the GDPR. 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 or by implementing the European Commission's standard contractual clauses with relevant supplementary measures. A copy of the relevant mechanism can be provided upon request, using the contact details provided at the end of this privacy policy.

We have offices in Sweden, the UK, Spain, Finland, Portugal, Malta, United States, Canada, Australia and Brazil. Employees and representatives for Trustly in these countries may, in case their job descriptions/tasks require so, access your personal data. Any personal data accessed from these locations is protected by EU data protection standards and is encrypted when transmitted over the Internet.

We undertake necessary measures to ensure that your personal data is protected with a high level of security that is appropriate to the risks associated with the processing and maintain physical, electronic, and procedural safeguards to protect it.

We restrict access to your personal data to those employees, Trustly representatives and third parties that need to know your information in order for us to be able to fulfil the purpose the data was collected for (see more under section 4 for more information).

We protect your information when transmitted over the Internet by using TLS-enabled services. The TLS-enabled services use industry best-practices configurations and adhere to industry-recognized standards.

8. Profiling and automated decision making

Trustly sometimes uses profiling and automated decision making when providing its services. In this section, you can read more about when and why we used these measures.

“Profiling” is when personal data is automatically processed for the purpose of evaluating personal aspects relating to an individual, for example a person’s economic situation or personal preferences.

“Automated decision making” is when automated means without human intervention are used for making a decision in relation to an individual, for example, automated denial of service.

You have the right to object to decisions based on automated individual decision-making, including profiling. How to object to these types of decisions is described below in section 9.

8.1. When you use our Service

When applicable, automated decision-making, including profiling, that may significantly affect you is decided when:

- Evaluating the risk of money laundering and the risk classification of potential and existing customers by screening your personal information against lists of politically exposed persons (“PEP”) and lists of persons subject to sanctions and other similar lists in accordance with anti-money laundering legislation to fulfil our legal obligations.
- Monitoring your payments processed by us to fulfil our legal obligation.
- Verifying your identity to ensure that you reside in a country where we offer our Service.
- Performing know your customer (“KYC”) checks, including conducting enhanced due diligence when applicable, in relation to verifying your identity and assessing your financial information.
- To prevent fraud and fraudulent activities.

The outcome of the automated decisions may be:

- Change of risk classification.
- Denial of service.
- Blocking of a customer and/or End-user.
- To block, hold or release transactions.

When providing our Direct Debit Payment service to you, we may use automated decision making and/or profiling for the purpose of verifying your identity to ensure that you reside in a country where we offer our Direct Debit Payment service and to assess risks related to your payments. When you use this service, the value of the Direct Debit Payments that you can request during a certain period of time is limited to a set amount. In case this limit is reached, we will instead automatically process your payment as a standard Pay-in.

The processing of your personal data in this automated decision making is carried out on the basis that it is necessary in order for us to fulfil our contractual obligations towards you to carry out payments or to comply with legal requirements, as the case may be. See section 5 for more information about whom we share information with, in regard to automated decisions, including profiling.

8.2. When you are a Customer representative

We may use profiling and automated decision making for the purpose of conducting know your customer checks, including performing enhanced due diligence when applicable, screening your personal information against PEP-lists and lists of persons subject to sanctions and other similar lists to assess implications of any money laundering risks. The processing of your personal data in this automated decision making is carried out on the basis that it is necessary in order for us to fulfil our contractual obligations towards the Merchant to provide the Service or to comply with legal requirements, as the case may be.

We may also use profiling to evaluate potential customer leads, for example by setting scores on you based on how much interest you have shown in Trustly, such as number of website visits, if you have signed up for information material on our websites, etc. The processing of your personal data in this profiling is based on our commercial legitimate interest of reaching out to potential or current customers of ours that have shown interest in Trustly and our Service.

9. Your rights

You have several rights in accordance with applicable data protection legislation. These rights are:

Right to withdraw your consent: If our processing of your personal data is based on consent, you have the right to withdraw your consent at any time. Information on how to withdraw your consent is included in connection with each description of our processing based on your consent.

Right to access your information: You can get information from Trustly about what personal data we have gathered, why we have gathered it, etc.

Right to rectification: If any of your personal data that we process is inaccurate, you are entitled to have it corrected.

Right to erasure ("right to be forgotten"): You can request that Trustly erase personal data that we have gathered about you. Trustly will, under certain circumstances, be obliged to remove it.

Right to restriction: You can request that Trustly restricts the processing of your personal data under certain circumstances, e.g. if you contest the accuracy of the personal data processed by us. We must then restrict the processing while verifying the accuracy of your request.

Right to object: You can object to the processing of your personal data that Trustly carries out based on the legal basis of our legitimate interest as specified above in this Privacy Policy, including profiling that we carry out on the basis of our legitimate interest, whereby we must assess if we can continue to process your personal data. You also have the right to object to processing of your personal data for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing, whereby your personal data will no longer be processed for such purposes.

Right to data portability: Where our processing is based on your consent or the performance of a contract, and the personal data in question has been provided by you, you can request that Trustly provides all the personal data that Trustly processes about you in a machine-readable format. In some cases, we are obliged to comply with that request and provide you with the personal data processed about you.

Right to object to automated decision making: You have the right to object to an automated decision made by Trustly, if the automated decision produces legal effects or similarly significantly affects you.

Lodge a complaint: If you are unhappy with our handling of your personal data, you can lodge a complaint to the Swedish Authority for Privacy Protection, which is the lead supervisory authority in relation to Trustly in the EU. You can also lodge a complaint with the data protection authority in your home country in the EU. If you are based in the UK, you can lodge a complaint to the Information Commissioner's Office in the UK.

10. Who to contact?

Trustly is responsible (data controller) for the processing of your personal data and has appointed a Data Protection Officer (DPO) who is responsible for monitoring our compliance with applicable data protection legislation. Trustly also has a dedicated privacy team, as well as a support team that can assist you in case of questions. If you want to reach any of us, have questions or want to exercise your rights explained above, you are welcome to contact us. Please do so by either sending a request to our support team by completing this online form <https://www.trustly.net/support/contact>, or send an email to our Privacy Team at privacy@trustly.com. If you want to reach our DPO specifically, please state this in your request or email.

11. Changes to this privacy policy

Please check this privacy policy every time you make a transaction using our Service, as updates may include information on additional processing activities we intend to perform going forward.