

Privacy Policy

This page presents the Transcepta Privacy Policy and describes how we use and protect personal information provided to us when you visit the Transcepta website, www.transcepta.com, or use our services through the [Transcepta Manager](#), [Transcepta Supplier Portal](#) and/or Transcepta's testing sites [Transcepta Manager Staging](#) or [Transcepta Supplier Portal Staging](#). Protecting your privacy is of critical importance to us, so we use stringent security measures to protect your personal information. We value your relationship and work hard to honor the trust you place in us. Thank you for choosing Transcepta.

How We Protect Your Privacy

Transcepta uses a combination of physical, electronic and procedural safeguards to help prevent unauthorized access to personal information and to protect it from loss, misuse, alteration or destruction. For example:

We limit access to our employees and other authorized parties who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs.

The information you provide to us online is protected by Secure Socket Layer (SSL) technology supporting up to 128-bit encryption to prevent unauthorized parties from viewing any personal information transmitted to or from Transcepta during your session. SSL is the leading security protocol for data transfer on the Internet. This technology scrambles your information as it moves between your PC's browser and Transcepta's computer systems. When information is scrambled, or encrypted in this way, it becomes nearly impossible for anyone other than Transcepta to read it. This secure session helps protect the safety and confidentiality of your personal information when you interact with us online.

We use other technological means (such as backup files, virus detection and eradication software, firewalls, and other computer software and hardware) to protect against unauthorized access or alterations to your data.

What Information We Collect

In the course of serving you, we collect information about you from a variety of sources, such as:

- Information you provide to us, such as your name, company name, addresses, phone numbers, email addresses, bank account and routing numbers, and passwords, and other information we need to perform services for which you have registered
- Information we receive from third parties, such as banking partners that may provide the status of payments from you or to you made via Transcepta
- Information your trading partners provide to us, such as your name, company name, addresses, phone numbers, email addresses and other information we need to initiate services with you
- Anonymous data our servers/web browsers automatically collect such as your IP address, your browser type, your operating system, and the timing and order in which our pages are accessed.

How We Use Information

Information collected may be used for a number of purposes, such as:

- Delivering invoices
- Processing electronic payments
- Enabling your electronic transfer exchange
- Confirming receipt of electronic transmissions
- Providing you your account history
- Contacting you about your account
- Performing other business activities as needed
- Keeping you informed about services or products that may be of interest to you
- Compiling anonymous statistical data and analysis for use internally or with third parties.

Why We May Disclose Information and to Whom

Transcepta always treats your personal information as confidential and takes all appropriate measures to protect it. We may disclose the information we collect as permitted by law and to nonaffiliated third parties such as:

- Companies that perform support services for us, such as technical systems consultants and programmers
- Companies involved in completing your transactions, such as financial institutions, your trading partners, fax transmitters or mail processors, or other business collaborators
- Fraud or identity screening services such as credit bureaus or other service providers to protect you and us against fraud

- Governmental agencies or authorities as required by law
- Third parties as required by law (in response to subpoenas or other legal processes), and those with whom you have requested us to share information
- If our business is sold or merged with another business, to the third-party acquiror of our business
- And we may disclose non-personally identifiable data to companies that use and analyze anonymous statistical data.

How We Use Tracking Technology

- To improve your experience
We may place cookies and similar files on your hard drive for security purposes, to facilitate site navigation, to facilitate your use of services, and to personalize your experience on our site. A cookie is a small text file assigned by a Web server to the browser on your computer that keeps track of your preferences and recognizes returning visitors. Cookies cannot be used to run programs or deliver viruses to your computer. Transcepta uses cookies to store your preferences and other information on your computer in order to save you time by eliminating the need to repeatedly enter the same information. When you sign in using your user name and password, the Transcepta Web server stores your unique identification, and the time you signed in, in an encrypted cookie on your hard disk. This cookie allows you to move from page to page on the site without having to sign in again on each page. When you sign out, these cookies are deleted from your computer. As a matter of security, we do not embed your account number(s) or passwords in our cookies.
- Website analytics
We may also partner with selected third-party vendors to allow tracking technologies and remarketing services on our site through the use of first party cookies and third-party cookies, to, among other things, analyze and track users' use of our site, determine the popularity of certain content and better understand online activity. By accessing our site, you consent to the collection and use of your information by these third-party vendors. You are encouraged to review their privacy policy and contact them directly for responses to your questions. We do not transfer personal information to these third-party vendors. However, if you do not want any information to be collected and used by tracking technologies, you can visit the third-party vendor or the [Network Advertising Initiative](#) or [Digital Advertising Alliance Opt-Out Tool](#).

We do not provide any personal information to an advertiser when you interact with or view a customized advertisement. However, when you view or interact with an

advertisement, the possibility exists that the advertiser will make the assumption that you are interested in the subject matter of the advertisements.

You should be aware that getting a new computer, installing a new browser, upgrading an existing browser, or erasing or otherwise altering your browser's cookies files may also clear certain opt-out cookies, plug-ins, or settings.

Third-Party Websites

Our site may contain links to third-party websites and applications of interest, including advertisements and external services, which are not affiliated with us. Once you have used these links to leave our site, any information you provide to the third parties is not covered by this Privacy Policy, and we cannot guarantee the safety and privacy of your information. Before visiting and providing any information to any third-party websites, you should inform yourself of the privacy policies and practices (if any) of the third party responsible for that website, and should take those steps necessary to, in your discretion, protect the privacy of your information. We are not responsible for the content or privacy and security practices and policies of any third parties, including other sites, services or applications that may be linked to or from our site.

Controls for Do-Not-Track Features

Most web browsers and some mobile operating systems include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. No uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this Privacy Policy.

How We Protect Information of Former Customers

We use the same stringent security measures to protect the personal information of our former customers as we do for our current customers.

California Users

If you are a California resident, under the California Consumer Privacy Act (“CCPA”), as may be amended from time to time, you may request up to two times in any twelve month period (1) that we disclose how we collect and use Personal Information as it relates to you, the categories of Personal Information we collect, the categories of sources we collect it from, and the categories of any third parties to whom we sell or disclose the Personal Information, (2) the specific pieces of Personal Information we collected about you during the prior 12 months, (3) to have such Personal Information corrected or deleted (with some exceptions), and (4) that your Personal Information not be sold or disclosed to third parties (although not disclosing it through the service to your approved trading partners or financial institutions or to our third-party providers means you will not be able to use portions of the service). We agree that we will not discriminate against you if you exercise any of these rights. Your request must be identified as a “Personal Information Request” and be directed to privacy@transcepta.com or call +1 (888) 221-2026. We will need to collect information from you in order to verify your identity, and then we will respond within 45 days of receiving your Personal Information Request. However, we cannot respond to your request or provide you with Personal Information if we cannot verify your identity and authority to make the request, and confirm that the Personal Information relates to you. Under the CCPA, as amended, Personal Information includes the personally identifying information identified in “What Information We Collect” above, as well as the following categories of information, some of which the law may deem to be “Sensitive Personal Information”, to the extent any is collected, (i) identifiers (such as cookie information), (ii) information protected against security breaches (such as name, driver’s license, social security number, user name and password); (iii) protected classification information (like race, gender, ethnicity), (iv) commercial information, (v) Internet/electronic activity, (vi) geolocation, (vii) audio/video data, (viii) professional or employment related information, (ix) education information, (x) biometrics, and (xi) inferences from the foregoing. We understand that California privacy regulations are amended from time to time, so we commit to comply with the most current privacy regulations that are applicable at the time you make a request pursuant to this paragraph.

European Union Users

The EU’s General Data Protection Regulation and related data protection law in Europe have special requirements for companies that collect and retain personal

information from citizens or residents of the European Economic Area. Even though Transcepta's service is a business-to-business service, users who work at the business may provide personal information, such as the person's business contact information, when signing up for the service and may also occasionally provide it in the invoices and other transaction documents exchanged with their trading partners and financial institutions through the service. Transcepta is deemed the "data controller" of any personal information provided to sign up for the service. Your or your trading partners and financial partners with whom you exchange documents through the service are deemed the "data controller" of any personal information you may include in your transaction exchange documents, as applicable under Transcepta's Terms of Service or your Agreement with Transcepta. In that case Transcepta is the "data processor" for you or your trading partners and/or financial partners, as applicable.

Transcepta is required to have a lawful basis for collecting and retaining personal information from citizens or residents of the European Economic Area. Transcepta's lawful basis includes:

- Performing the business-to-business transaction document exchange services and any other services your business has signed up for pursuant to an agreement with Transcepta, and to manage your account with us.
- Legitimate interests that are permissible under the data protection regulation and related laws, for which we have a good and fair reason and which are done in ways that would not hurt your interests or rights, such as would be expected as part of running our services or business. For example, managing your account with us, to follow your instructions, to share your information with your trading partners and financial institutions to facilitate processing your transactions, to keep our services secure and to prevent fraud, to communicate with you, to send you information about our services (subject to your right to control whether we do so), to analyze how our services are being used and to improve and develop our services, and in connection with any changes in our business, such as a sale or merger.
- Legal compliance.
If you are a user in the European Economic Area and Transcepta is the "data controller", you may contact us at as indicated below to request information from us regarding what personal information of yours we may hold, to access it, to correct or update it, in certain circumstances to delete it, and to object to our use or disclosure of it. If you are a user in the European Economic Area and Transcepta is the "data processor", we may refer your request to your trading partner or financial institution that is the "data controller" and cooperate with their handling of the request. You also have the right to lodge a complaint with the relevant supervisory

authority, but we encourage you to first contact the applicable data controller to resolve your concern.

Changes to This Privacy Policy

We may occasionally update this Privacy Policy to reflect changes in our services. If we post changes to this Privacy Policy, we will revise the “last updated” date at the bottom of this statement. If there are material changes to this statement or in how Transcepta will use your personal information, we will notify you either by prominently posting a notice of such changes prior to implementing the change or by directly sending you a notification. We encourage you to periodically review this statement to be informed of how Transcepta is protecting your personal information.

Questions and Suggestions

Transcepta welcomes your comments. If you have any questions regarding this Privacy Policy or believe that we have not adhered to it, please contact us as indicated below.

info@transcepta.com

(Last updated 5.31.2023)