

**BeyondTrust Privacy Notice**

Last Update: September 13, 2024

**Purpose of this notice**

At BeyondTrust, we are committed to safeguarding your privacy and protecting your personal information. This privacy notice provides you with the necessary information regarding your privacy rights and our obligations. Here we explain how, why and when BeyondTrust process your personal data when you use our website, services, or products. This includes any data you provide via our website when you purchase any products or services, request a trial, or register for a marketing event.

It is important that you read this privacy notice together with any other notice we may provide on specific occasions when we are processing personal data about you. In this way you can be fully aware of how, why and when we are using your data. This privacy notice supplements any other notices and is not intended to override them.

We recommend that you read this Privacy Notice in full to ensure you are fully informed. We have provided links to specific sections below to assist in finding specific information relevant to you.

[Contents](#)

- Purpose of this notice ..... 1
- Who we are and what we do..... 1
- What information we collect, how and why..... 2
- Who do we share your personal data with.....12
- Your Privacy Rights.....13
- Data Security .....14
- How long we keep your personal information for .....15
- International Data Transfers.....15
- Consumers in the USA.....17
- Children’s Personal Data .....18
- Changes to this Notice.....18
- Contact Us.....19

**Who we are and what we do**

BeyondTrust Corporation and its corporate affiliates (referred to as “BeyondTrust”, “we”, “us” or “our”) offer intelligent identity and secure access products and services.

We are the controller of your personal data and we are responsible for processing it according to the law.

Our principal office is at 11695 Johns Creek Parkway, Suite 200, Johns Creek, Georgia 30097 and we are a U.S. corporation registered in Delaware. For more information on our global offices, see our [Contact](#) page.

**Data Protection Officer (DPO):** We have appointed a DPO who is responsible for answering questions about this privacy notice and the processing of your personal data. If you have questions, including any requests to exercise your rights, please contact our DPO, Valerie Moulden, at [dataprotectionofficer@beyondtrust.com](mailto:dataprotectionofficer@beyondtrust.com).

### **What information we collect, how and why**

BeyondTrust processes different categories and types of personal data about you when you navigate our websites or use our services and products. In this section you will find:

- the categories and types of personal data we process about you
- the purpose and the lawful ground for processing your data
- an explanation of how we collect your personal data

We have also included some useful definitions to help you understand this section better.

<p><b>What is personal data?</b></p> <p>Personal data, or personal information, is any information that, either alone or in combination with other information, enables us to identify you. It does not include any data where the identity has been removed (ie anonymous data). Please note that the definition of personal data or personal information may change depending on the applicable law.</p>
<p><b>What is processing?</b></p> <p>Processing means any operation that is performed on your personal data. It can be done manually or by automated means, and it includes the following operations: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction.</p>

### **Categories and types of personal data we process**

<p><i>Technical data</i></p>	<p>Your browser type and version, your operating system/platform and other technology on the devices you use to access our websites, your Internet service provider and IP address, the date and time you access our website as well as time zone settings and location, and date and time you register to our newsletter or similar marketing subscription.</p>
------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<i>Usage data</i>	Information about how you use our website, products and services, details of websites from which you have accessed our website, and details of websites you access from our website (for example, where you click on a link from our websites).
<i>Marketing and communications data</i>	Your preferences in receiving marketing from us and our third parties and your communication choices.
<i>Contact information</i>	Your full name, your work and/or home address, work, home or mobile telephone number, personal or professional email address, and job title.
<i>Identity data</i>	Your user ID or username and your password.
<i>Financial and transactional data</i>	Your product and service purchases and preferences, your bank account information, your payment card information, and your billing address. Some of this information may be collected through our payment services provider's website.
<i>Conversational data</i>	Recording and transcripts of certain calls and email exchanges between customers or prospects and BeyondTrust representatives.
<i>Profile data</i>	Your interests, preferences, feedback and survey responses.
<i>CCTV/Camera footage data</i>	Footage from security cameras in the BeyondTrust offices where these are installed.

### **On what lawful grounds do we process your personal data?**

Privacy laws allow companies to process personal data of individuals like you when there is a legal justification (legal basis) for doing so. The main legal basis we use to process your personal data are:

<i>Consent</i>	You give clear consent for us to use your data.
<i>Contract performance</i>	Processing your data is necessary to carry out a contract between us, or if you ask us to take steps to enter into a contract with you.
<i>Legitimate interests</i>	We process your personal data based on our legitimate interests, or the legitimate interests of a third party. However, these interests must not be outweighed by your rights, freedoms or interests.
<i>Legal obligation</i>	We must process your personal data because it is required by law.
<i>Vital interest of individuals</i>	We need to process your personal data to protect your vital interests. For example, if you or another person need medical emergency care.

### **Why and on what lawful grounds we process your personal data**

<b>Access and use of our websites:</b>	
<i>Purpose/Activity</i>	The processing of certain technical data, including IP addresses, by our systems is necessary for you to access the websites. It is essential that we keep this information for the duration of your session. This information is also stored in the log files of our system, and we have measures in place to ensure that it is not stored together with other personal data of the user.
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Technical data</li> <li>• Usage data</li> <li>• Marketing and communications data</li> </ul>
<i>Lawful Basis</i>	<u>Legitimate interests</u> : to run our business, identify types of customers for our products and services, providing you information on our products and services, keep our website updated, relevant and secure, develop our business and inform our marketing strategy.
<b>To process your inquiries, online trials and demos requests:</b>	
<i>Purpose/Activity</i>	When you inquire about or order products or services on our website or in other ways, we may ask you to provide personal data to complete these transactions and provide you the relevant products and services. We store this data in our central customer database to fulfil your inquiries, process relevant contracts (including payment processing and, if applicable, credit assessment), and for our own advertising purposes (see below for more information). Payment card information is only used for processing payments and decisions as to whether to offer credit and fraud prevention.
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Contact information</li> <li>• Identity data</li> <li>• Financial and transactional data</li> </ul>
<i>Lawful Basis</i>	<u>Contract performance</u> : We need to process your personal data under the terms of a contract we have with you. This also includes when you ask us to take certain steps before entering into a contract. If you fail to provide the data when requested, we may not be able

	<p>to perform the contract we have or are trying to enter into with you. In this case, we may have to cancel a product or service you have with us but we will try to notify you if this is the case at the time.</p>
<p><b>Direct marketing activities:</b></p>	
<p><i>Purpose/Activity</i></p>	<p>We process your personal data to send you marketing communications (e.g. via email, social media, or telephone) and product and services recommendations.</p> <p>When you subscribe to our free newsletter on our website, you provide us with personal data via the online form. We also ask you about your marketing preferences when you purchase any products or services. In addition, we may automatically collect personal data upon your registration.</p> <p>We would like to keep you informed about new products, our services and interesting events. To do this, we use your personal data to recommend certain of our products, services or events that may be of interest to you by email or post. To provide more relevant information to you, we may process data relating to your purchase history. We will only use your data for our own marketing and advertising purposes and do not transfer any personal data to third parties for marketing purposes.</p> <p>If you purchase, take a trial of, or express interest in any of our products or services via our website, we may also send you a newsletter to the contact details you provide. Our newsletter will only advertise our products or services that are similar to those that you have purchased, trialled or in which you have expressed interest, provided that you have not opted out of receiving that marketing.</p> <p>If you do not purchase or trial any of our products or services, but wish to subscribe to our newsletter, we ask you to consent to us</p>

	<p>processing your personal data for these purposes and we reference this privacy notice during the registration process. We do not pass this personal data to third parties. We only use it to send you our newsletter. You have the right to withdraw your consent and stop receiving marketing communications and newsletters at any time by contacting us or using our <a href="#">marketing preference centre</a>.</p> <p>We also partner with third party advertising networks to display advertising on our website or to manage our advertising on other sites. Our advertising network providers may collect information about your activities on our website and other websites to provide personalised advertising based on your interests. You can find more information in our Cookie Notice.</p>
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Contact information</li> <li>• Transaction data</li> <li>• Marketing and communications data</li> <li>• Technical data</li> </ul>
<i>Lawful Basis</i>	<p>We send you marketing communications if you provide us with your <u>consent</u>. However, we may also rely on our <u>legitimate interests</u> to study how customers use our products or services, to develop our business practices and inform our marketing strategy, as well as to contact you about services or products similar to the ones you may have already purchased, discussed, or trialled.</p>
<b>Use of microsites to collaborate with prospects and customers</b>	
<i>Purpose/Activity</i>	<p>We use a third party service to create microsites which can be shared externally to centralise tools, resources and information and increase collaboration and work effectively with prospects and customers.</p>
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Technical data</li> <li>• Contact information</li> </ul>

<i>Lawful Basis</i>	<u>Contract performance</u> : We need to process your personal data under the terms of a contract we have with you. This also includes when you ask us to take certain steps before entering into a contract. However, we may also rely on our <u>legitimate interests</u> to work more collaboratively with you and allow you to access tools, resources and information more efficiently.
<b>Partner relationship management:</b>	
<i>Purpose/Activity</i>	We use Salesforce.com as a Partner Relationship Management (PRM) tool. We use this to give our referral and reseller partners access to our sales and marketing materials. We also allow them to submit leads for deal registration and to view their existing sales opportunities with us.
<i>Type of Personal Data</i>	Contact information
<i>Lawful Basis</i>	<u>Contract performance</u> : We need to process your personal data under the terms of a contract we have with you. This also includes when you ask us to take certain steps before entering into a contract. Further, it is necessary for our <u>legitimate interests</u> for running our business, and for providing you information on our products and services.
<b>Surveys and contests:</b>	
<i>Purpose/Activity</i>	We may provide you the opportunity to participate in voluntary contests or surveys on our websites. We will process your personal data only if you participate. We may use a third party service provider to conduct these surveys or contests. We will not share the personal data you provide in a contest or survey with other third parties, unless we notify you of this in advance.
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Contact information</li> <li>• Profile data</li> </ul>
<i>Lawful Basis</i>	For surveys, our <u>legitimate interests</u> to study and analyse how customers use our products and services, to develop them and grow our business.

	For contests, we process your data when you <u>consent</u> .
<b>Use of our product and services:</b>	
<i>Purpose/Activity</i>	When you purchase our services or products, we process your personal data to set up your account, provide and maintain the service, support you when you ask and send you administrative communications. However, note that when you are submitting personal data in our services, products, or applications you are acting as data controller, and we will act as data processor, as provided in the relevant agreement in place with you as a customer.
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Contact information</li> <li>• Identity data</li> <li>• Financial and transactional data</li> </ul>
<i>Lawful Basis</i>	Our lawful basis for the processing of this data is that it is necessary for the <u>performance of a contract</u> with you, as well as for our legitimate interests to provide and administer our service. Please note that we may need to collect certain personal data by law, or under the terms the a contract we have with you to provide you with our services. If you fail to provide the data when requested, we may not be able to perform the contract we have with you. In this case, we may have to cancel a product or service you have with us but we will try to notify you if this is the case at the time.
<b>Use of Password Safe plugin:</b>	
<i>Purpose/Activity</i>	If you use our Password Safe browser plugins in your browser, we process your personal data to provide you with the plugin and its functionalities. We will also process certain metadata about your credentials.
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Technical data</li> <li>• Identity data</li> </ul>
<i>Lawful Basis</i>	Our <u>legitimate interests</u> to provide you with the plugin and its functionalities.
<b>Registration in BeyondTrust University:</b>	

<i>Purpose/Activity</i>	If you are a customer or a partner and you register in our University portal, we will process your personal data for to create your account. When using the portal, you can join challenges and keep track of your progress with courses and classes. When doing so, your full name may be visible to other registrants that joined the same challenge.
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Contact information</li> <li>• Identity data</li> </ul>
<i>Lawful Basis</i>	Necessary for the <u>performance of a contract</u> between us, and necessary for us to provide the requested service.
<b>Use of customers telemetry data to improve the product:</b>	
<i>Purpose/Activity</i>	When you use our products or services, we process certain telemetry data to provide you a better service. Specifically, we use this data to measure, support and improve our products. We will only process this data when you authorize us.
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Technical data</li> <li>• Usage data</li> </ul>
<i>Lawful Basis</i>	Our <u>legitimate interests</u> to measure the way customers use our products to provide them with a better service and support.
<b>Call recording and transcript:</b>	
<i>Purpose/Activity</i>	If you are a customer or a prospect, we may record and transcribe certain calls and email exchanges you have with BeyondTrust representatives, for the purpose of product improvement and employee skills development. We will do this only if you consent to it.
<i>Type of Personal Data</i>	Conversational data
<i>Lawful Basis</i>	If you provide your <u>consent</u> before the call takes place.
<b>Registering visitors</b>	
<i>Purpose/Activity</i>	If you visit one of our offices, we will identify you, provide you with a visitor badge and ask you to sign our guest book in and out of the office.
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• Contact information</li> </ul>

<i>Lawful Basis</i>	Our <u>legitimate interests</u> to have visibility over who enter our offices, for security and safety reasons.
<b>Securing our physical offices</b>	
<i>Purpose/Activity</i>	If you visit one of our offices, you may be recorded by the security cameras installed in some of our offices. We installed security cameras to ensure the safety of our physical offices. Visible signage will be in place, so you will be aware of when and where you may be recorded.
<i>Type of Personal Data</i>	<ul style="list-style-type: none"> <li>• CCTV/Camera footage data</li> </ul>
<i>Lawful Basis</i>	Our <u>legitimate interests</u> to ensure the security and safety of our physical offices.

## How we collect your personal data

### Data you send to us

You may provide us with your information by filling in forms or by corresponding with us. This includes personal data you provide when you:

- Apply for our products or services
- Create an account or register as a referral and reseller customer
- Subscribe to our newsletter or other similar services
- Request marketing communications or materials
- Apply for a job
- Enter a contest or respond to a survey, or otherwise provide feedback

### Data we collect automatically

We automatically collect information during your visit to our websites, newsletters, discussion forums and lists and opt-in announcement lists (the "BeyondTrust Network"). We do this via our automatic data collection tools ("Data Collection Tools"), such as cookies, web beacons, embedded web links, and other commonly used tracking technologies.

These Data Collection Tools collect technical and usage data that your browser sends to our websites such as your browser type and language, access times, and the address of the website from which you arrived at the BeyondTrust Network. These Data Collection Tools may also collect information about your IP address, clickstream behavior and product information. When a visitor requests a page from any website within the BeyondTrust Network, our web servers automatically recognize that visitor's domain name and IP address.

We collect and use your IP address and cookie information to better understand your needs and interests to help deliver a consistent and personalized experience on the BeyondTrust Network. We will only use your IP address to the extent necessary to protect our legitimate interests or

the legitimate interests of a third party (this may include pursuing legal claims and investigating criminal offences).

You can adjust your cookie preferences [here](#). For more information on our use of cookies and similar tracking technologies, visit our Cookie notice.

### Third parties and publicly available information

We also collect information from credible, third party, and commercially-available sources. The information we collect from these sources may include your name, phone number, business address, email address, firmographic data, which may be used along with the information we collect when you visit the BeyondTrust Network.

### **Aggregated data**

We also collect, use, and share aggregated data such as statistical or demographic data for different purposes. Aggregated data may be derived from your personal data but is not considered personal data according to applicable law, as this data does not directly or indirectly reveal your identity, and instead relates to a number of individuals. For example, we may aggregate your usage data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

### **Special categories of personal data**

#### **What are special categories of personal data?**

Special categories of personal data are also called sensitive data. They are personal data that deserve a stronger protection because of their sensitive nature. For example, the following are sensitive personal data:

- race and ethnic origin
- religious or philosophical beliefs
- sex life and sexual orientation
- political opinions
- trade union membership
- health information
- genetic and biometric data

We do not generally collect any special categories of personal data about you. We also do not collect any information about criminal convictions and offences, except for background checks we perform on job applicants to whom we would like to offer a position. See our Candidate Privacy Notice for more information.

### **Additional information**

We will only use your personal data for the purposes for which we collected it. However, if we reasonably consider that we need to use it for another reason that is compatible with the original

purpose, we may do that. You can contact us if you want an explanation of how the processing for the new purpose is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do. If we need, we will ask your consent. However, we may process your personal data without your knowledge or consent, where this is required or permitted by law.

## **Who do we share your personal data with**

We will only share your personal data with external subjects in these circumstances:

### **Third party service providers**

We use service providers to deliver our products, services and customer solutions and to assist us with marketing and other communications. These providers include, for example, payment processors, providers of customer support and live-help services, email service providers, automated data processors, and shipping agents. We require all service providers to keep your personal data confidential, to respect the security of your personal data and treat it in accordance with the law.

### **Third party acquirer**

If we sell, transfer, or merge parts of our business or our assets to third parties, we may share your personal data with them. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, the new owners may use your personal data in the same way as set out in this privacy notice. If there is such a change in ownership, we will notify you as soon as practicable.

### **Other third parties**

We may also share your personal data with external third parties in these cases:

- to comply with any applicable law, regulation, subpoena, or court order.
- to respond to authorized information requests of police and governmental authorities.
- to protect the safety of our employees and third parties on our property.
- to answer lawful access requests by public authorities, including to meet national security or law enforcement requirements (for more information, see our Government & Law Enforcement Request Policy and Transparency Report).
- To help prevent fraud or to enforce or protect our rights and properties.

### **Third-party links**

Our website includes links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy notices.

When you leave our website, we encourage you to read the privacy notice of each website you visit.

## Your Privacy Rights

You have many rights under applicable data protection laws in relation to your personal data. We listed your privacy rights in the table below.

You can exercise your rights by contacting us at [dataprotectionofficer@beyondtrust.com](mailto:dataprotectionofficer@beyondtrust.com) or at the other contacts provided at the end of this notice. When you contact us, please include sufficient information to confirm your identity and deal with your request, such your name, surname, and email address. This is a security measure to ensure that your personal data is not disclosed to someone with no right to receive it.

We will respond to all legitimate requests in one month (or by the timeframe provided by applicable law). Occasionally it may take us longer if your request is particularly complex or you have made a number of requests. In this case, we will notify you, explain the reasons, and keep you updated.

You also have the right to complaint to the relevant supervisory authority for data protection. We would, however, appreciate the chance to deal with your concerns before you approach the supervisory authority. Please contact us in the first place.

If you are a USA resident, see the "Consumers in the USA" section below for more information about your rights.

<b>Access your personal data</b>	You can request access to your personal data. This enables you to confirm if we are processing your personal data and receive a copy of the same.
<b>Objection against advertising</b>	You can object to the use of your personal data for advertising purposes at any time. Do one of the following: <ul style="list-style-type: none"><li>- select the "opt out" or "unsubscribe" link in the email, or follow the opt-out instructions included in each communication; or</li><li>- contact us at <a href="mailto:dataprotectionofficer@beyondtrust.com">dataprotectionofficer@beyondtrust.com</a> or at the other contacts listed at the end of this notice.</li></ul>
<b>Withdrawal of consent</b>	Where we rely on your consent to process your personal data, you can withdraw such consent at any time. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent.
<b>Correction of your personal data</b>	You can request the correction of any of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected. Note that we still may

	need to verify the accuracy of the new personal data that you provide to us.
<b>Data deletion</b>	<p>You can ask us to delete or remove your personal data. Some examples of when you could ask for it:</p> <ul style="list-style-type: none"> <li>- where there is no good reason for us continuing to process it.</li> <li>- where you have successfully exercised your right to object to processing (see the next privacy right).</li> <li>- where we may have processed your personal data unlawfully.</li> <li>- where we are required to erase your personal data to comply with applicable law.</li> </ul> <p>Please consider that we may not always be able to comply with your deletion request for specific legal reasons, which will be communicated to you, if applicable.</p>
<b>Objection of processing of your personal data</b>	<p>Where we rely on a legitimate interest to process your personal data, you can object to this processing. For example, you may ask us to stop processing your personal data because you feel it impacts your rights and freedoms in a particular situation.. When you object, we will no longer process your personal data in this way, unless we can demonstrate that we have compelling legitimate grounds to process it, which outweigh your rights and freedoms.</p>
<b>Restriction of processing of your personal data</b>	<p>You can ask us to suspend the processing of your personal data in the following cases:</p> <ul style="list-style-type: none"> <li>- if you want us to establish the accuracy of your personal data.</li> <li>- where our use of your personal data is unlawful but you do not want us to delete it.</li> <li>- where you need us to hold your personal data even if we no longer require it as you need it to establish, exercise or defend legal claims.</li> <li>- you have objected to our processing of your personal data but we need to verify if we have overriding legitimate grounds to use it.</li> </ul>
<b>Data portability</b>	<p>You can ask us to transfer your personal data to you or to a third party. We will provide you, or the third party, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to personal data we processed in an automated way on the basis of your consent or to perform a contract with you.</p>

## Data Security

We have appropriate physical, technical and administrative data security measures to protect your personal data. This allows to prevent unauthorized access, use or disclosure, to maintain data accuracy, and to ensure the appropriate use of your personal data. However, no method of transmission over the Internet, or method of electronic storage, is 100% secure. We have procedures in place to deal with any suspected data breach, and will notify you and/or any competent authority of a breach where it is legally required. For more information on our security program and certifications, visit our [Security page](#).

### **How long we keep your personal information for**

We will only keep your personal data for as long as necessary to fulfil the purposes we collected it for. This includes the purposes of satisfying any legal, accounting, or reporting requirements. We consider different factors to determine the appropriate retention period for personal data. For example, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes of processing and if we can achieve those purposes in other ways, and the applicable legal requirements.

### **International Data Transfers**

BeyondTrust is an organization based in the US and operating globally. We may transfer your personal data outside of your country of residence or presence to where we or our service providers operate (you can see a list of our affiliates and sub-processors here). No matter where your personal data may be transferred, we will always protect it as described in this privacy notice.

When we transfer personal data originating from the EU, the UK, or Switzerland, we use the following transfer mechanisms:

- Adequacy decisions, as adopted by the competent regulators ([EU Commission](#), [UK Secretary of State](#), or [Swiss data protection authority](#)); or
- [EU Standard Contractual Clauses \(SCCs\)](#), as amended or recognized by respectively the UK and Swiss regulators.

BeyondTrust carries out transfer impact assessments (TIAs) before transferring EU, UK, or Swiss personal data internationally. We also monitor the circumstances of the transfers, to ensure that the personal data is granted a level of protection substantially equivalent to the one provided under EU, UK, or Swiss law.

Where we transfer personal data originating from other countries, we rely on one of the transfer mechanisms provided by the applicable law in the given country. This may include, among others, an adequacy/equivalence decision, data transfer agreements, or your consent to the transfer.

## Data Privacy Framework Notice

BeyondTrust complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. BeyondTrust has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. BeyondTrust has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

BeyondTrust is committed to processing personal data transferred from the EU, UK and Switzerland in compliance with the EU-U.S. Data Privacy Framework Principles, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework Principles, listed below:

- Notice
- Choice
- Accountability for Onward Transfer
- Security
- Data Integrity and Purpose Limitation
- Access
- Recourse, Enforcement and Liability

If there is any conflict between this privacy notice and the Data Privacy Framework Principles, the Data Privacy Framework Principles prevails.

BeyondTrust is responsible and liable for the processing of data it receives, under the Data Privacy Framework, and subsequently transfers to a third party acting as an agent on its behalf. BeyondTrust complies with the Data Privacy Framework Principles for all onward transfers of personal data from the EU, UK and Switzerland, including the onward transfer liability provisions.

The Federal Trade Commission has jurisdiction BeyondTrust's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF). In certain situations, we may be required to disclose EU or Swiss personal data in response to lawful requests by US public authorities, including to meet national security or law enforcement requirements. To learn more about the

Data Privacy Framework and view our certification, visit the U.S. Department of Commerce's [Data Privacy Framework List](#).

In compliance with the EU-U.S. DP, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, BeyondTrust commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU, UK and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF should first contact BeyondTrust at: [dataprotectionofficer@beyondtrust.com](mailto:dataprotectionofficer@beyondtrust.com).

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, BeyondTrust commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to TRUSTe, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit <https://feedback-form.truste.com/watchdog/request> for more information or to file a complaint. The services of TRUSTe are provided at no cost to you.

Under certain conditions, that are fully described in [Annex I of the DPF Principles](#), you may invoke binding arbitration for complaints regarding DPF compliance not resolved by any of the other DPF mechanisms.

## **For Consumers in the USA**

This section applies if you are a California or Virginia resident. In this case, the California Consumer Privacy Act (CCPA) or the Virginia Consumer Data Protection Act (CDPA) apply to our processing of your personal information.

In the past 12 months, BeyondTrust collected the categories of personal information provided in the *“What information we collect, how and why”* section above. In that section, you can learn about the sources from which your personal information was collected, as well as our business or commercial purpose of collection.

In the past 12 months, we also disclosed some of yours personal information for a business purpose with affiliates, third parties, and service providers, as listed in the *“Who do we share your personal data with”* section above.

We do not “sell” (as defined under CCPA and other US privacy laws) your personal information to other businesses or third parties for monetary consideration. However, we may share it with third parties for other non-monetary considerations. This could be considered a “sale” under CCPA or other US privacy laws.

We do not sell personal information of consumers under 16 years of age.

## **Your rights**

You have the following rights under CCPA and CDPA:

Right to know about the personal information we collect about you and how it is used and shared. This includes the right to request that we disclose:

- the categories of personal information and sources of the same
- the specific pieces of personal information we collected about you
- our business or commercial purpose for collecting, selling, or sharing your personal information
- the categories of your personal information that we sold or disclosed for a business purpose and the categories of third parties to whom we sold or disclosed such information in the preceding 12 months

Right to delete personal information we collected (under some exceptions).

Right to opt-out of the sale or sharing of your personal information to third parties. Please visit our “Do Not Sell or Share my Personal Information” page to exercise this right.

Right to non-discrimination for exercising your CCPA rights. We do not offer promotions, discounts or other deals in exchange for collecting, keeping, or selling your personal information.

To exercise these rights contact us at [dataprotectionofficer@beyondtrust.com](mailto:dataprotectionofficer@beyondtrust.com), or at one of the contacts provided in the “Contact Us” section below. You can also designate someone else (authorized subject) to make a request on your behalf. We will however confirm the subject’s identity and require a written authorization. Requests made by your authorized subject should be made to the contacts indicated above.

Virginia Right to Appeal. You can appeal our decision about your request to exercise your rights, if you disagree. To do this, send your appeal to [dataprotectionofficer@beyondtrust.com](mailto:dataprotectionofficer@beyondtrust.com) within a reasonable time from when we sent you our initial decision. We will consider your appeal and answer within 60 days (or the different period provided by law), explaining the reason of our final decision. If we deny your appeal, we will tell you how you can contact the competent Attorney General to submit a complaint, if you wish.

### **“Do not track” notice**

We do not respond to ‘do not track’ signals or similar mechanisms.

### **Children’s Personal Data**

We are a B2B organization directed to adults. Our website and services are not intended for individuals under the age of 13 (or the equivalent age for minors under applicable law). We also do not knowingly collect children data. If we learn that we collected a child’s personal data, we will delete it as soon as possible. If you become aware that a child has provided us with personal data, contact us at [dataprotectionofficer@beyondtrust.com](mailto:dataprotectionofficer@beyondtrust.com).

### **Changes to this Notice**

We may update this privacy notice to reflect changes to our privacy and security practices. If we make any material changes, we will provide notice on our website as soon as practicable and, if possible, before the change becoming effective. We encourage you to periodically review this privacy notice for the latest information on how we process your personal data. You can access archived versions of this Privacy Notice and read a summary of the latest changes [here](#).

## Contact Us

<b>Email</b>	<a href="mailto:dataprotectionofficer@beyondtrust.com">dataprotectionofficer@beyondtrust.com</a>
<b>Address</b>	11695 Johns Creek Parkway, Suite 200, Johns Creek, Georgia 30097. You can also find our global offices in our <a href="#">Contact</a> page.
<b>Telephone</b>	1-877-826-6427

We will process your privacy enquiries as soon as practicable in accordance with our legal requirements and, if appropriate, inform you which measures we have taken.