

Privacy Notice

“Remarkably Human” is one of the core principles Asurion’s culture strives towards and is front of mind in the way we handle and protect your personal data. With that goal in mind, we are providing this Privacy Notice (“Notice”) to describe how Asurion collects, uses, discloses, and handles your personal data, and information about privacy rights you may have, depending upon where you live.

A Few Terms

When we use “Asurion”, or terms like “we”, “us”, or “our” in this Notice, we’re referring to Asurion, LLC and our subsidiaries and affiliates.

When we use terms like “you” and “your,” we’re talking about you as a visitor to our websites that refer to this Notice or as a user of Asurion products and services.

When we refer to “personal data,” we mean any information that relates to an identified or identifiable person, whether that person is identifiable directly or indirectly.

Scope of this Privacy Notice

This Notice applies to the personal data we collect when you visit this website and visit or use any of our other websites or mobile applications that reference this Notice, or when we interact with you in other ways in providing and marketing our products and services to you, including at a physical location such as a corporate store. If you are looking for information about how we collect personal data from our employees or applicants, please review the [Asurion Employee Privacy Notice](#).

It is important to understand that this Notice applies only when Asurion controls how and why your personal data is being used, such as when you visit our websites or use our applications or make purchases directly from Asurion.

When Asurion is providing products and services on behalf of and at the direction of one of our corporate customers, those services may be provided under those customers’ privacy notices and policies instead of, or in some cases in addition to, this Notice. If you have questions about uses of your personal data by an Asurion corporate customer, they should be directed to the company through whom you may have encountered Asurion.

Supplemental Notices

In some special cases, Asurion may provide a product or service offering that includes a supplemental privacy notice that gives additional information about that offering's use of personal data. In that situation, if anything in the supplemental notice conflicts with information provided in this Notice, the supplemental notice's information controls. If there are supplements, links to such notices may be found at the end of this Notice.

Accessibility

If you are visually impaired, you may access this Privacy Notice through your browser's audio reader.

Sources of Personal Data

We collect personal data about you from a variety of sources. Some information comes directly from you (or people/entities acting on your behalf) during the course of your interactions with Asurion, such as when you visit our websites, use our applications, file a claim, create a user account, purchase products and services, request information or otherwise communicate with us, interact with our support teams or other staff, or participate in Asurion events.

We may also gather information about you from other sources, including:

- **Public Sources**, including information from public records and information shared in public forums, including social media;
- **Social Media Networks**;
- **Your Mobile Devices and Other Electronics** involved in your interactions with Asurion, including the operating systems and platforms they use; and
- **Other Third-Party Sources**, including corporate customers we partner with and other partners we engage to help us prevent fraud, develop and enhance products, and support our marketing and promotion activities.

We may combine information that we receive from these different sources and use or disclose it for the purposes described below.

Categories of Personal Data We Collect

We may collect the following categories of personal data about you, depending on your relationship or interactions with Asurion.

- **Identifiers** including contact information like your name, physical address, phone number and email address, identifying information about your device, such as the International Mobile Equipment Identity (IMEI) number, and similar numbers.
- **Location Data**, such as approximate location based upon your IP address and more specific longitude and latitude coordinates, used to verify your identity and for fraud prevention purposes.
- **Commercial Information**, such as purchase history, preferences, and transactional information, and records of interactions created in providing services and support to you, such as support notes or chat histories.
- **Financial Information** such as payment card information collected by our payment processors on our behalf or, in some cases, collected directly from you.
- **Internet or Other Electronic Network Activity Information**, such as IP addresses, unique device identifiers, browsing session data, and other similar information.
- **Device Information**, including unique identifiers for electronic devices, technical or diagnostic information and other data we may need to interact with you or provide service for your device. This includes any information you provide to us to access your device for servicing. In some cases, photographs of your device before and after repair may be necessary for insurance claims.
- **Fraud Prevention Information**, including data used to help identify and prevent fraud, including fraudulent claims and fraudulent or criminal customer impersonation.
- **Audio and Visual Information** such as audio recordings of interactions we may have with you and video recordings or photographs at our stores and other physical sites.
- **Inferences**. We draw inferences from the personal data we collect to develop a profile reflecting preferences and characteristics relevant to our interactions with you.
- **Demographic Information**, such as information about your gender, age, level of education, and/or occupation.

- **Identification Documentation.** Where permitted or required by applicable law, we may require information to validate your identity, such as a copy of your driver's license, passport, or other personal identification card.
- **Information From On-Site Services.** If Asurion provides services to you in your home or another remote location, the service provider may be able to view anything visible to visitors in your home, which may include personal data.
- **Other Information You Choose to Share.** Some Asurion products or services such as Asurion Photos may include a storage component that permits you to save information, files, or media of your choosing. Subject to the terms of use of such offerings, the nature and volume of personal data you choose to upload (if any) is entirely up to you, and Asurion makes no use of any such personal data except to provide the service or product that includes this component.
- **Special Note for Users of Asurion Photos' Facial Detection Feature.** Asurion Photos offers a feature that includes technology that permits users of the application to organize pictures by recognizing faces in the user's photo collection and allowing the user to group photos that contain similar faces. Use of this feature may create data considered to be biometric identifiers or biometric information under some laws. Your use of this feature is optional, and the feature is turned off by default. It is always your choice whether to enable or disable the feature. Asurion makes no use of any of the information generated by this feature except for the purpose of providing the service to you.
- **Special Note for Users of Asurion LeakProtect.** Asurion LeakProtect offers a service through which Asurion coordinates the installation of a device that detects anomalies in water pipe flow that can indicate a leak. In the event of an alert, Asurion could shut off water flow to your home remotely. You control whether Asurion has the ability to perform this function. In order to provide LeakProtect services, Asurion collects and processes personal data like your address and other Identifiers, home insurance details, water usage, and photos of water pipes on your property. Asurion may share your information we collect under this program with your insurance company.

Asurion does not knowingly collect personal data of individuals under the age of 18. Our website(s), mobile apps and services are not designed for children under 18, and we do not intentionally or knowingly collect personal data from users who are under the age of 18 or from other websites or services directed at children. If we discover that a child under 18 has provided us with personal data, we will delete such information.

Cookies and Other Tracking Technologies

We use several types of tracking technologies (e.g., cookies, web beacons, pixels, and device identifiers) to provide functionality, to recognize you across different services and devices including for the purposes of advertising and re-engaging you if you have searched for, viewed, and/or purchased our products or similar products, and to improve your experience. Asurion gives you control over which of these cookies, pixels or other technologies (other than those essential to the functioning of the website) are used with your interactions with us via the Asurion Privacy Preference Center, which can be accessed by clicking the “Cookie Preferences” button that appears at the bottom of the Asurion.com homepage. Learn more about how we use [cookies and tracking technologies here](#).

Asurion.com recognizes the Global Privacy Control

Asurion.com now recognizes the Global Privacy Control (“GPC”), which enables us to automatically honor your cookie preferences as expressed through a browser or plug-in that uses the GPC without the need for you to make a separate effort to express those preferences. You can find out more about the GPC, how it works, and different ways you can use the tool at <https://globalprivacycontrol.org/>.

How We Use Your Data

In general, we use your data to respond to requests that you make, to process claims or to aid us in serving you better. Some jurisdictions where we operate require businesses/data controllers to specify the legal basis for processing of personal data. We rely on the legal basis as described below.

Providing our products and services to you. This data is processed for the performance of a contract to which you are a party and in some instances, it is necessary for our legitimate interests or to comply with legal requirements. This may include:

- Activating, authenticating, and maintaining your account;
- Operating, maintaining, and supporting our offerings to you;
- Processing claims you may make;
- Communicating with you, including offering you updates, notices, and invitations to participate in surveys;
- Tracking service or quality issues; and

- Improving our offerings.

Supporting our day-to-day business operations. This data is processed for the performance of a contract to which you are a party and in some instances, it is necessary for our legitimate interests or to comply with legal requirements. This may include:

- Maintaining internal business records;
- Internal reporting;
- Auditing, accounting, and payment collection functions;
- Administration of our systems and networks;
- Research and development;
- Customer relationship management;
- Business planning and other activities associated with managing, analyzing improving and developing our business; and
- Corporate transactions, such as mergers and acquisitions.

Managing legal and operational risks., This data is processed for the performance of a contract to which you are a party and in some instances, it is necessary for our legitimate interests or to comply with legal requirements. This may include:

- Maintaining the security and integrity of Asurion's systems and services;
- Protection of our physical facilities and digital assets;
- Prevention of fraud and other illegal activity;
- Complying with laws; and
- Establishing, exercising or defending against legal claims.

Marketing our products and services., This data is processed with your consent if required by law and in some instances, it is necessary for our legitimate interests. This may include:

- Providing you with information about Asurion offerings we think may interest you, as permitted by law;
- Facilitating customer-oriented events;
- Evaluating and improving the effectiveness of our marketing efforts and strategies;
- Continuous improvement of your experience as an Asurion customer; and
- Tailoring advertising that we believe may be of greatest relevance to you.

How We Disclose Your Personal Data

We may disclose your personal data as follows:

- To business partners and service providers to support our business purposes, as more fully described in “How We Use Your Data”
- Among Asurion affiliates and subsidiaries, as appropriate for the purposes set forth above.
- Where required by law or legal process, to enforce or protect Asurion’s rights under the law, or where otherwise appropriate and permitted by law to prevent harm, loss, or suspected illegal activity.
- In the context of an actual or prospective business transaction involving all or part of our company, including mergers, acquisitions, consolidations or divestitures.

We may combine data we collect from different contexts (for example, from your purchase of multiple Asurion products) to give you a more seamless, consistent, and personalized experience, to make informed business decisions, and for other legitimate purposes.

Some of the activities described above could involve use of AI tools or services to process your personal data. These AI tools and services could be developed by Asurion’s vendors, or developed by Asurion itself. Some Asurion services include customer-facing AI tools, such as chatbots, where you may interact directly with an AI. The purposes for which your personal data is processed by these tools will follow this Notice.

The categories of personal data we may disclose in any of these scenarios will vary depending upon what is necessary in a given situation but may include any of the categories of information described in “Categories of Personal Data We Collect” above.

Should we need to use your personal data for a purpose not previously disclosed, or share it with an external party not covered by this Notice, Asurion will offer you the opportunity to opt out.

How We Protect Your Personal Data

We have a robust security program that uses appropriate technical, administrative, and physical controls to protect your personal data against accidental or unlawful destruction, loss, disclosure, alteration or use. We also require this of our vendors and business

partners, as in some circumstances Asurion could be liable for these parties' processing activities.

Prior to engaging any third-party service provider, Asurion performs due diligence to evaluate their privacy and security practices.

If permitted by current contractual relationship, Asurion may transfer your personal data outside of your country. When doing so, we will comply with applicable regulatory and contractual obligations to protect your data where it is transferred.

How Long We Keep Your Personal Data

The amount of time we retain a particular category of personal data will vary depending on the purpose for which it was collected, our business need for it and our legal obligations with respect to it. We retain your personal data for the time needed to fulfill the purpose for which that information was collected, to meet any legal obligations, and to adhere to our policies on keeping records.

Exercising Your Rights Under Privacy Laws

Depending upon where you reside, you may have certain rights related to your personal data, including rights to access, correct, limit use or disclosure, data portability, and, in some cases, request deletion of your personal data. You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is unfounded or excessive.

If we used consent to lawfully and fairly use your personal data, you may withdraw your consent at any time. In some cases, we may limit or deny your request to withdraw consent if the law permits or requires us to do so, or if we are unable to adequately verify your identity. Requests to exercise these rights can be submitted through [Asurion's Privacy Rights Portal](#), or by calling [1-844-798-7701](tel:1-844-798-7701). Asurion will respond to these requests in the manner prescribed by law.

Asurion will take reasonable steps to validate your identity before responding to a privacy rights request. The information required from you to validate your request will usually be information like your name, email address, or other similar contact information. In some cases, additional personal data may be needed from you to validate your identity. Asurion reserves the right not to respond to requests generated through third-party applications or

automated processes without direct validation of the requests by individuals using the resources provided by Asurion for the exercise of these rights.

Privacy Framework Certifications

TRUSTe APEC Certification

Asurion maintains TRUSTe APEC certifications for the Cross Border Privacy Rules (CBPR) system and Privacy Recognition for Processors (PRP). You may find information about APEC generally [here](#).

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our US-based third-party dispute resolution provider at [TRUSTe](#). Dispute resolution procedures could include binding arbitration.

EU-US Data Privacy Framework Certification

Asurion complies with the EU-US Data Privacy Framework (EU-US DPF) and the UK Extension to the EU-US DPF as set forth by the US Department of Commerce. Asurion has certified to the US Department of Commerce that it adheres to the EU-US Data Privacy Framework Principles (EU-US DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-US DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-US DPF. If there is any conflict between the terms in this privacy notice and the EU-US DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit [Data Privacy Framework website](#).

The DPF is issued by the US Department of Commerce. Asurion is likewise subject to the investigatory and enforcement powers of the US government, including the US Department of Commerce and the US Federal Trade Commission. In certain situations, Asurion may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In the context of onward transfers, Asurion is accountable for the processing of personal data it receives under the EU-U.S. DPF and the UK Extension to EU-U.S. DPF, and subsequently transfers to a third party acting as an agent on its behalf. Asurion remains liable under the EU-U.S. DPF Principles, and the UK Extension to the EU-U.S. DPF if Asurion's agent processes personal information in a manner inconsistent with the EU-U.S.

DPF Principles, and the UK Extension to the EU-U.S. DPF, unless Asurion proves that it is not responsible for the event giving rise to damage.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, Asurion 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 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.trustarc.com/watchdog/request> for more information or to file a complaint. These dispute resolution services are provided at no cost to you.

For complaints regarding EU-U.S. DPF, the UK Extension to the EU-U.S. DPF compliance not resolved by any of the other DPF mechanisms, you have the possibility, under certain conditions, to invoke binding arbitration. Further information can be found on the official DPF website: <https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2>.



External Links

This Notice does not cover third-party websites or applications that may be linked from our services. By linking to third-party services, we do not imply an endorsement.

It is a good practice to review the privacy notice of any third-party website or application that collects your personal data.

Changes to this Notice

We update this Notice periodically to comply with global laws and regulations and our changing business practices. You will find the date of the most recent update at the top of the current Notice. Please visit this site periodically to read the Notice. We will comply with applicable laws to the extent they require any additional means of alerting you to changes to the Notice.

Where to Turn with Questions and Complaints

You can contact Asurion’s Privacy Office with questions about this Notice or the use of personal data related to our websites, products, or services, or contact our data protection officer, by sending an email to privacy@asurion.com or by calling [1-844-798-7701](tel:1-844-798-7701), or by mail at:

Asurion
c/o General Counsel
cc: Asurion Privacy Office
140 11th Ave. North
Nashville, TN 37203

You may also have the right to lodge a complaint with the UK Information Commission, [click here](#), or a European Economic Area supervisory authority, [click here](#). However, if you have a complaint regarding the processing of your personal data, we request that you first contact Asurion Data Protection Officer [here](#) or as indicated above and we will reply promptly.

Information for California Residents

This portion of the Notice pertains to personal data we collect from or about California residents and provides additional information required by California law.

California-Designated Categories of Personal Data We Collect The categories of data Asurion collects are described above in “Categories of Personal Data We Collect.” Although we have sought to present a clear and accurate summary of the data we collect in that section, California regulations designate specific category titles to be used in describing the data. A summary of those categories and how they correspond to the information previously described appears below.

California Designated Categories	Corresponding Categories Above
Identifiers	Identifiers
Geolocation Data	Location Data
Commercial Information	Commercial Information
Financial Information	Financial Information

Internet or Other Electronic Network Activity Information	Internet or Other Electronic Network Activity Information
Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information	Audio and Visual Information
Inferences	Inferences
Characteristics of Protected Classifications under California or Federal Law	Demographic Information
Professional or Employment Information	Demographic Information
Sensitive Personal Information	Identification Documentation
Biometric Information	Special Note for Users of Asurion Photos' Facial Detection Feature

Sensitive Personal Information

Some of the categories listed above include information that California designates as “sensitive personal information.”

We do not use or disclose sensitive personal information except as follows:

- Where necessary to perform services for or provide products to you;
- In detecting security incidents, and protecting against malicious, deceptive, fraudulent or illegal activity and responding to such activity;
- Short-term transient uses where permitted by law;
- Where needed for services to be provided for us to accomplish ordinary business purposes, such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage; or
- Where needed to verify or maintain the quality or safety of our products and services.

"Selling" and "Sharing" of Your Personal Data

California law defines the terms “selling” and “sharing” in a manner that differs from what the words typically mean in common conversation. Asurion does not sell your personal data for money. However, within the last 12 months, we have engaged third parties who

support our marketing activities and disclosed personal data to them in a manner that may be considered a “sale” under California law.

Under California law, “sharing” is defined as providing or communicating an individual’s personal data to a third party for purposes of cross-context behavioral advertising. Asurion has shared personal data for these purposes within the last 12 months, including as described in “Cookies and Other Tracking Technologies” above.

In the case of both “selling” and “sharing” within the meaning described here, the personal data disclosed falls into the categories of 1) identifiers, 2) internet or similar network activity, and 3) inferences from personal data, and the third parties to whom we have disclosed such information assist us in providing, maintaining and operating our marketing activities.

Asurion does not sell or share personal data that California defines as “sensitive personal information.”

As noted above, Asurion does not knowingly collect personal data about individuals under the age of 16 and therefore does not sell or share such information.

Information About California Privacy Rights

Residents of California have specific and enumerated rights to control and understand their personal data. These rights include:

Right to Know You may request information about what categories of personal data we have about you, the categories of sources from which we collected that information, the purposes for collecting that personal data, the categories of third parties to whom we have disclosed your personal data, and the purposes for which the data was disclosed. You may also request specific pieces of personal data that we have about you.

Right to Delete You may ask that Asurion delete any of the personal data that we possess about you, subject to certain exceptions.

Right to Correct Your Personal Data You may request that Asurion correct any personal data we have about you that you believe to be incomplete or inaccurate.

Requests to exercise these rights can be submitted through [Asurion’s Privacy Rights Portal](#), or by calling 1-844-798-7701. Asurion will respond to these requests in the manner

prescribed by law, including your right not to be discriminated against for exercising these rights.

Opt Out of Sharing you may opt out of sharing of your personal data by clicking on the “Cookie Preferences” link on the button on our homepage to access the Asurion Privacy Preference Center and toggling off targeting cookies and tracking technologies. As noted above, Asurion.com also honors cookie preferences signaled by the Global Privacy Control. Please be advised that should you choose to disable certain tracking technologies, you may encounter functionality issues with some of our sites.

Authorized Agents

A properly authorized agent may be able to exercise California privacy rights on your behalf. Authorized agents must contact us by submitting a request through our webform and indicate that they are submitting the request as an agent. We reserve the right to require the agent to validate their identity and to require the agent to demonstrate authority to act on your behalf by providing signed permission from you. We may also require you to verify your own identity directly with us or to directly confirm with us that you provided the authorized agent permission to submit the request.

Statistics for Asurion’s Responses to California Privacy Rights Requests

California regulations require that Asurion provide statistics regarding the number of data subject requests we received, fulfilled, and/or denied in the previous calendar year. These are presented in the table below for 2025.

Request Type	Received	Fulfilled	Denied	Denial Reason(s)
Know	14	10	4	Unable to validate identity within a reasonable time
Delete	155	2	153	Legal/Regulatory Requirements; Required to provide service; Unable to validate identity within a reasonable time
Correct	3	0	3	Unable to validate identity within a reasonable time
Opt-Out of Marketing	23	17	6	Unable to validate identity within a reasonable time

We responded to these requests within a mean time period of 8 days.