

Last updated: 14 May 2018

We value privacy, especially yours

At Asurion, we understand the importance of protecting your privacy. We want you to understand what personal information (also known as personal data) we collect, why it is collected, how it is used, and other important information so that you are informed and there are no surprises.

This policy is incorporated as part of the terms of any agreement that you have with Asurion that applies to your use of the services.

If you do not agree to the terms of this policy, please do not use our services or provide any personal information.

If you fail to provide certain information when requested, we may not be able to provide the services for which you have contracted, such as processing a claim.

Data Controller

The controller of your personal information is Asurion Europe Limited with its registered offices at Chiswick Place, 272 Gunnersbury Avenue, Chiswick W4 5QB ("Asurion").

Asurion Europe Limited is also authorised and regulated in the United Kingdom by the Financial Conduct Authority ("FCA") under FCA register number 502545. Asurion is registered with the Information Commissioners Office as a Data Controller (number Z2176995).

Why we collect your personal information and the purpose of processing

Personal information we collect when you use our services is needed for the following purposes:

Contract: to communicate with you, process enrollments, bill and collect, process cancellations, process claims that you submit, provide customer service, administer your policy, and manage our supply chain management to deliver replacement devices to you.

Legitimate interests: for maintaining our books and records, maintaining security and integrity, monitoring use and performance, quality assurance, fraud detection and prevention, and product improvement and development.

Comply with legal requirements: to notify you as required by law in the event of a breach regarding the security of your personal data. We also use your personal information to comply with any other UK or EU legal requirements.

Where to turn with questions

Please contact our Data Protection Officer by postal mail or email anytime.

Asurion
Attn: EU Data Protection Officer
c/o Office of the General Counsel
648 Grassmere Park
Nashville, TN, USA 37211

privacy@asurion.com

What's covered by this policy

Any Asurion-affiliated site or service(s) that links to this policy

This policy does not cover and we are not responsible for third-party sites or applications that may be linked from our sites; linking to them does not imply an endorsement. We are not responsible for these sites or applications or any information they may collect. You should always review the privacy policy of any third-party site or application.

Personal information we collect

When you use our services, we may collect the below types of personal information:

- Name;
- Mailing address;
- Email address;
- Mobile phone number and information that identifies your mobile device, such as an IMEI;
- Information collected after obtaining your permission;
- Any information that you provide as part of filing a claim;
- Information provided by your mobile network provider to validate your claim;
- Other information that personally identifies you or is linked or linkable to you.

As part of the claim process, Asurion or its affiliates may require you to provide a copy of your driver's license, passport or other forms of identification. Additionally, in order to process your claim, Asurion or its affiliates may request your shipping and billing information, credit card information or other preferred payment means.

Asurion and its partners use cookies or similar technologies to analyse trends, administer the site, track users' movements around the site, and to gather demographic information about our user base as a whole.

Asurion also gathers certain information about the use of Asurion's services, including the number of unique visitors, the frequency of visits, how users interact with the sites, user experience preferences, IP address, and other information that may help Asurion improve the customer experience, mitigate fraudulent activity, and comply with legal requirements. Such information may include, but is not limited to the following:

Log information

When you visit Asurion's sites we automatically collect and store certain information in our server logs. This type of information includes details of how you interacted with our services. It may include personal information such as: IP address, Unique Device Identifier, or CallerID / ANI (Automatic Number Identification) information, content of web pages, transaction with APIs (Application Program Interface), transactions with IVR (Interactive Voice Response) systems, activity and content of visitor interaction with call center representatives; application usage activity, hardware information, hardware and system settings, browser type, browser language, the date and time of your request, referral URL, etc.

Cookies

A cookie is a small, data file that is managed by your web browser or other application and stored on your local system. Asurion uses session and persistent cookies to, among other things, identify your computer during a particular interaction and analyse your behavior during a particular visit. Most web browsers provide you with the ability to accept or decline cookies, as well as to be warned each time a cookie is being sent. If you choose to decline cookies, you may not be able to fully use Asurion's services. You can find more information about cookies at allaboutcookies.org and youronlinechoices.eu.

Pixel tags

Pixel tags, also known as web beacons, help Asurion better manage user experience and content tracking. Pixel tags are tiny graphics with a unique identifier, which provide a similar function to cookies and are used to track user interaction with content provided by Asurion or an affiliate organisation. In contrast to cookies, which are stored on a user's computer hard drive, pixel tags are embedded invisibly within content. The small size and transparency of pixel tags are not intended to deceive content recipients, but minimise distraction.

Third-party data sources

Asurion may leverage external data sources in order to provide context and background on the users of its services in order to improve customer experience, mitigate fraud or malicious activity, or comply with internal company and external regulatory requirements.

How we share your personal information

We will not use or disclose your personal information to third parties except as disclosed in this policy.

Asurion may transfer your personal information to:

Non-affiliated companies that include telecommunication carriers, credit card payment processors, security service providers, service providers who send communications on our behalf and third parties providing claims fulfillment, supply chain logistics, data center operations, information technology, customer service and quality assurance monitoring. These companies are required to comply with the principles set out in this policy and only use such personal information for the purposes for which it was provided to them;

A third-party, in the event of a proposed or actual purchase, sale (including a liquidation, realisation, foreclosure or repossession), lease, merger, amalgamation or any other type of acquisition, disposal, transfer, conveyance or financing of all or any portion of its business or of any assets or shares of our business or a division thereof in order for you to continue to receive the same or similar products and services from the third-party. In these circumstances, personal information may be shared with the actual or prospective purchasers or assignees, or with the newly acquired business.

How long we keep your personal information

To determine the appropriate retention period for personal information before we securely destroy it, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

How you are notified if the policy changes

We may change this policy from time to time. If we do, we will post the updated policy with the last revised date. You acknowledge that your continued use of our services after we publish or send a notice about our changes to this policy means that the collection, use and sharing of your personal data is subject to the updated policy. You should periodically read the policy to understand our privacy practices.

How we will communicate with you

We will communicate with you by SMS, email or in writing using your given contact details. We will also send certain communications by SMS to the mobile number associated with your airtime contract.

Individuals under the age of 18

Our services are not directed to, and we do not knowingly collect personal information from, individuals under the age of 18. If a child is accessing services without your consent, please contact us by using the information provided below so that we can remove any personal information provided.

Transferring personal information from the EU

Personal information we collect from you may be processed by Asurion and third-parties as described in the “How we use your personal information” section in the United States and other countries and used consistent with your relationship with Asurion and the practices described in this policy.

Personal information will only be transferred to locations outside of the UK and the EU where permissible legal structures exist or where the country is deemed “adequate” by the EU Commission.

Security of your personal information

We have implemented technical and organisational measures designed to provide appropriate levels of security for your personal data. Reasonable administrative, logical, and physical controls are in place to prevent your personal information from being accidentally lost, used, or accessed in unauthorized ways.

Accuracy of personal information and your individual rights

While we take various steps to ensure the accuracy and completeness of your personal information, we rely upon you to provide accurate and complete personal information when interacting with us.

Your rights in connection with your personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a ‘data subject access request’). This enables you to receive a copy of the personal information we hold about you.
- **Request correction** of any incomplete or inaccurate personal information that we hold about you.
- **Request erasure** of your personal information when there is no need for us continuing to process it or you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- **Request the restriction of processing** of your personal information to suspend the processing, for example if you want us to verify its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to exercise any of these rights, please contact the Data Protection Officer in writing per the [Where to turn with questions](#) section at the end of this Notice. Valid requests will be honored within 30 calendar days of request. This 30-day period may be extended for another 2 months for complex requests with notification of the reasons for the extension to you. Any such requests should be submitted to the Data Protection Officer.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances. In addition, there may be requests that we are unable to process because of other EU legal requirements. If a request is denied, we will notify you of the reason.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

You also have the right to lodge a complaint with the UK Information Commissioner's Office or other EU supervisory authority. However, if you have a complaint regarding the processing of your personal information, we request that you first contact the Asurion Data Protection Officer as indicated in the [Where to turn with questions](#) section of this policy and we will reply promptly.

APEC participation

The Asurion privacy practices, described in this policy, comply with the APEC Cross Border Privacy Rules System. The APEC CBPR system provides a framework for organisations to ensure protection of personal information transferred among participating APEC economies. More information about the APEC framework can be found [here](#)

To learn more about our APEC CBPR Certification click [here](#).