

Union Assurance Privacy Policy

Union Assurance PLC knows that it is important to you to be able to maintain your privacy while visiting our website. It is in our mutual interests that we take our responsibility to guarantee the privacy of your data very seriously, in compliance with the applicable provisions of data protection law. We use state-of-the-art technology to communicate with you while keeping your data secure.

Scope of application

The following data protection notice applies to Union Assurance's internet presence. This website contains links to Union Assurance applications.

2. Use of your data

We would hereby like to explain how your personal data will be processed when you visit Union Assurance website, and to inform you of your rights under data protection law.

2.1. Who will be responsible for processing your data, and how can you reach the Data Protection Officer?

Union Assurance Centre,
20, St. Michael's Road,
Colombo 03, Sri Lanka.

Tele: +94 11 2990990
Telefax: +94 11 2438165
E-Mail: unionassurance@ualink.lk

You may contact our Information Security Officer at the aforementioned address, or via the e-mail address itservicedesk@ualink.lk.

2.2 What categories of data will we use, and for what purposes do we process personal data?

You are generally free to visit our website anonymously. Union Assurance does not save any personal or traceable data (e.g. IP addresses) of visitors to its website. We collect impersonal data about visits to our website (date, time, pages visited, navigation, software used) to have user habits anonymously analysed by an external service provider. The data is rendered anonymous before it is saved by the service provider.

If you disclose your personal data to us in specific circumstances (for example, by filling out a contact form), we handle such data confidentially, in accordance with the data protection regulations in effect at our Company's registered office. If you send us an e-mail, or if you complete and submit an on-line form on our website, we will use any personal data you provide (such as your name or e-mail address) only to correspond with you, to send you the information you requested, or for the other purpose(s) stipulated on the particular form.

For legal or technical reasons, personal data may also be collected and communicated to us in an encrypted form from areas on our website that are accessible only to users with special authorization (for example, the shareholder portal or job application portal). The amount of data collected depends on the application used.

For every application or process with which we collect your personal data, we will provide an individualised privacy statement to inform you about the processing of your data.

2.3 What is the legal basis for our processing of your personal data?

We process your data on the basis of the provisions of the Electronic Transactions Act No. 19 of 2006, Payment Devices Frauds Act No 30 of 2006, the Intellectual Property Rights Acts, and Computer Crimes Act No 24 of 2007 and all other laws applicable to the processing of personal data. The substantive legal grounds for the processing depend on the context and the purpose for which we collect your data.

As a rule, we collect and process your personal data to communicate with you and send you the information that you request. This may be necessary, in the context of a contractual relationship, to fulfil a contract or during the pre-contractual process (for example, job application process), or at your request. Where the applications are restricted-access (for example the job applicant portal), the user or data subject's consent may constitute the legal grounds. You may revoke such consent at any time.

Within Union Assurance PLC, only those staff and departments who are responsible for the respective process will receive your data. The data may also be disclosed to service providers for the purposes set out above. Using service providers is necessary, for example, for the administration and maintenance of our IT systems. We also use external service providers for support when managing job applicants, for example. If we process any of your personal data for certain purposes, you will receive a notice about how exactly your data is being used.

Service providers that we use to send you the requested information (such as brochures by mail, issuing newsletters) will receive your required personal data (e.g. postal services receive your name and address).

A list of all service providers that we use for data processing can be found under Section 3, and also is available for downloading.

2.4 What measures do we have in place to protect your data?

We have state-of-the-art technical and organisational security measures to protect data against accidental or intentional manipulation, loss, destruction, and access by unauthorised parties. We use Secure Socket Layer (SSL) encryption to protect any information you enter in dialogue forms on our web pages. SSL encryption protects your data against unauthorised third-party access during transfer. You can recognise an encrypted connection by the change in your browser address line from `http://+` to `https://+`, and the padlock symbol appearing in your browser window.

For your own security, please always use our contact forms. If you send us unencrypted data in a normal, unprotected e-mail, it is possible that unauthorised parties may gain knowledge of or modify your data during transmission via the internet.

2.5 What data protection rights can you claim as a data subject?

At the address indicated above, you may request information about the personal data we have stored under your name. In addition, under certain conditions you may request that your data be deleted or corrected. Furthermore, you may also have a right to restrict the processing of your data and a right to disclosure of the data you have made available in a structured, common and machine-readable format.

2.6 Right to object

If we process your data for the purposes of safeguarding legitimate interests, you may object to this processing on grounds relating to your particular situation. We will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms, or if the processing serves the assertion, exercise or defense of legal claims.

2.7 How long will your data be stored?

We will delete your personal data as soon as it is no longer required for the purposes set out above, and no legal documentation or retention requirements apply.

2.8 Who can you contact if you have a complaint?

If you have a complaint, you may contact the aforementioned Information Security Officer.