

Assured Guaranty

Bermuda Privacy Notice

Effective Date: March 27, 2025

Bermuda's data protection legislation, the Personal Information Protection Act 2016 ("**PIPA**") became effective 1 January 2025. This privacy notice ("**Bermuda Privacy Notice**") supplements the global [Privacy Policy](#) of Assured Guaranty Ltd. (together with its affiliates and subsidiaries, "**Assured Guaranty**", "**we**", "**us**", or "**our**") and applies to personal information that is collected by or on behalf of Assured Guaranty and is used in Bermuda. We separately address personal information relating to our staff, job applicants and independent contractors.

This Bermuda Privacy Notice is intended to provide individuals with clear and easily accessible information about our practices and policies with respect to your personal information that we use in Bermuda. It does not confer any contractual right on you or place any contractual obligation on us.

We may update or otherwise amend this Bermuda Privacy Notice at any time.

1. Definitions

- "**Personal information**" means any information about an identified or identifiable natural person.
- "**Use**" or "**using**", in relation to personal information, means carrying out any operation on personal information, including, but not limited to: collecting, holding, organising, altering, transferring, disclosing, combining, blocking, erasing or destroying it.
- "**Sensitive personal information**" means any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.

2. How we collect your personal information

Much of the information we hold will have been provided by you. We may also collect your personal information from various other sources including third parties, for example, through cookies, pixels, web beacons and other similar data collection and tracking technologies. We also collect information through our systems – e.g. IT and email systems and CCTV footage (as described later in this Bermuda Privacy Notice).

3. Your personal information that we use and how we use it

The Company may directly and indirectly collect and use all or some of the following types of personal information (including sensitive personal information):

Assured Guaranty collects and maintains the following categories of personal information:	Assured Guaranty collects this personal information for the following purposes:
<ul style="list-style-type: none"> • Vendor information (where the vendor, or their representative, is a natural person), including for example: <ul style="list-style-type: none"> ○ Contact details such as name, address, e-mail address and telephone number ○ Banking information to process payments 	<ul style="list-style-type: none"> • Administer our contract/engagement with you and/or the vendor you represent
<ul style="list-style-type: none"> • Information about those who visit our Bermuda office(s), including for example: <ul style="list-style-type: none"> ○ Name, the name of their company (if relevant), office access data (including times of entering and leaving) and CCTV footage 	<ul style="list-style-type: none"> • Ensuring the physical security of Assured Guaranty's premises, property and purposes • Ensuring the safety of our visitors • See below for more information about our monitoring processes
<ul style="list-style-type: none"> • Information about natural persons relating to our transaction counterparty data, including for example: <ul style="list-style-type: none"> ○ Contact name, business email address and contact number, date of birth, passport number/copy of passport, residential address for purposes of know-your-client (KYC) and other compliance checks 	<ul style="list-style-type: none"> • Ensuring appropriate counterparty due diligence is performed to comply with anti-money laundering, sanctions and anti-terrorist financing regulatory requirements.

To the extent permitted by applicable laws, we may also collect and process a limited amount of personal information falling into special categories, called “sensitive personal information”.

We have set out above a summary of how we might use your personal information. We will use the information only when we have a lawful basis to do so. For example, we may also need to use your personal information where it is necessary in order for us to comply with a provision of law that authorises or requires such use.

We may ask for your consent to certain processing. We shall provide clear, prominent, easily understandable, accessible mechanisms for you to give consent in relation to the use of your personal information, unless it can be implied from your conduct that you consent to the use of your personal information (excluding sensitive personal information) for the intended purposes of which we have notified you. Where consent is given, it may be withdrawn by you at any time, but this will not impact on any other lawful basis for processing relied on by the Company. In some cases your refusal may mean that we're unable to continue providing you our services as we may not have the personal information we believe necessary for the effective and efficient administration and management of our relationship with you.

4. Monitoring

Any usage of company computer and communication systems, including email, internet facilities and, in some areas, phone lines, may be subject to monitoring in compliance with law and best practice. For example, we may

monitor your usage: to prevent, detect or investigate suspected misconduct, illegal conduct, wrongdoing or other misuse; to comply with legal obligations; or to locate and retrieve lost messages or files.

Email, voicemail messages, recordings and internet usage are potentially subject to interception and to disclosure to third parties in the course of litigation or an investigation. We have a legitimate basis on which to access and protect company data stored or processed on a device, including the content of any communications sent or received from the device.

Our offices use CCTV, internally and externally, and you may be recorded when visiting and/or working from our premises. We use the CCTV footage for security purposes, and to prevent, detect or investigate suspected misconduct, illegal conduct, wrongdoing or other misuse.

When entering our offices and premises you will be required to provide us information about you for our security purposes, and so that we can ensure your safety and security while visiting us.

5. Retention Periods

We will keep your personal information no longer than is necessary for the purpose of its use, including in accordance with any statutory or regulatory requirements and our record retention policies. A limited and reasonable amount of information will be kept for archiving purposes, for example; and even where you have requested we no longer keep in touch with you, we will need to keep a record of the fact in order to fulfil your wishes.

The Company's retention periods for the personal information we use is generally impacted by the following criteria: (i) the purpose for which we are processing your personal information (we need to retain the information as long as is necessary for that purpose); and (ii) legal obligations (laws or regulation may set, or recommend, a minimum period for which we have to, or should, keep your personal information).

6. Who has access to your personal information

Your personal information will only be used and disclosed as permitted by applicable law, and may be shared within the Assured Group if required.

For the most part, personal information collected by us will remain within the Assured Group, and will be accessed and used by appropriate individuals only in accordance with our access protocols (e.g. on a 'need to know' basis).

We may share your personal information with third parties. For example:

1. To our external legal counsel, banks, auditors, shareholders, consultants and other professional advisors
2. Other service providers, such as security and IT providers
3. Government or regulatory authorities as requested by such authorities or required by applicable law

This could relate to, for example, our complying with our statutory obligations in light of imminent or pending legal proceedings or a statutory audit of the company.

Your personal information is also accessed by third parties with whom we work together in connection with IT services, such as hosting, supporting and maintaining the framework of our information systems. Data contained in such systems may be accessible by providers of those systems, their associated companies and sub-contractors.

Some of these transfers will include transfers overseas. For example:

- Foreign banks if you receive overseas payments
- To our overseas lawyers and professional advisors
- To foreign government or regulatory authorities as requested by such authorities or required by applicable law

Where your personal information is transferred to a third party located outside of Bermuda, we will take steps to ensure that your personal information is adequately protected and transferred in accordance with any applicable data transfer requirements.

7. Security safeguards that we use

We use commercially reasonable administrative, technical, and physical safeguards to protect your personal information from loss, misuse, and unauthorized access, disclosure, alteration, or destruction, for which we take into account the nature of the information (including its sensitivity and context), its processing, and the threats and potential harm posed to it. Unfortunately, no data transmission or storage system can be guaranteed to be secure at all times. If you have reason to believe that your interaction with us is no longer secure, please immediately notify us via email at security@agltd.com with the subject line “Security Concern” or call +1 212-893-2760.

8. Your rights in relation to your personal information

You have certain rights with respect to your personal information and how it is used in Bermuda, as set forth below. For more information about these rights, or to submit a request, please email us at privacy@agltd.com with the subject line “PIPA Request.” If you make a request, we will respond to you within the time frame(s) required by applicable data protection laws and guidelines. Please note that in some circumstances we may not be able to fully comply with your request, such as if it is manifestly unreasonable, if it jeopardizes the privacy, life or security rights of others, or if it is not required by law, but in those circumstances, we will still respond to notify you of such a decision. In some cases, we may also need you to provide us with additional information, which may include personal information, if necessary to verify your identity and the nature of your request.

- **Rights of access:** You can request access to your personal information that is in our custody or control, the purposes for which the personal information has been and is being used by us and the names of the persons or types of persons to whom and circumstances in which the personal information has been and is being disclosed
- **Rights to correction:** You can request that we correct an error or omission in any of your personal information which is under our control
- **Rights to restriction of processing:** You may request that we cease, or do not begin, using your personal information where the use of that personal information is (i) for the purposes of advertising, marketing or public relations and/or (ii) causing, or is likely to cause, substantial damage or substantial distress to the individual or to another individual
- **Rights to erasure and destruction:** You can request that we erase or destroy your personal information where it is no longer relevant for the purposes of its use.

Any request must be in writing and provide sufficient detail to enable us to identify the personal information to which the request relates.

We will respond to all requests we receive from individuals wishing to exercise their PIPA rights in accordance with applicable data protection laws. We reserve the right to keep any information in our archives that we deem necessary to comply with our legal obligations, resolve disputes and enforce our agreements. Please note that all of these rights are subject to applicable exemptions and restrictions and are not absolute rights. If we need to rely on these exemptions or restrictions, we will provide this information to you in our response.

9. Contacting Assured Guaranty & our Privacy Officer

Our organisations in Bermuda, who use personal information in Bermuda, include Assured Guaranty Ltd., Assured Guaranty Re Ltd., Assured Guaranty Re Overseas Ltd. and Cedar Personnel Ltd., whose offices are located at 30 Woodbourne Avenue, Hamilton HM 08, Bermuda.

If you have any questions about this Bermuda Privacy Notice or to request more details about your rights and how we handle your personal information, please contact privacy@agltd.com.

You can also contact our Privacy Officer at bermudaprivacyofficer@agltd.com.

10. Bermuda Privacy Notice updates

This Bermuda Privacy Notice is subject to change in accordance with changes to applicable laws or our internal policies and procedures. The date below indicates when this Bermuda Privacy Notice was last revised.

Any changes to this Bermuda Privacy Notice will be effective upon publication of the revised notice.

Version Control

Version	Date	Approved by	Comment
1.0	March 27, 2025	Dana Damiani, Privacy Officer	Privacy Notice (External – Online) implemented pursuant to PIPA requirements