

Assurant Employee Privacy Statement

This Employee Privacy Statement ("Statement") applies to individuals who reside in the United States or Puerto Rico and who engage with one or more Assurant legal entities ("Assurant", "we", "our") for employment-related purposes whether as an employment applicant, employee, director, or independent contractor. For all other countries, contact your People Organization Representative for guidance on the privacy notice applicable to your country.

This Statement does not apply when you interact with Assurant in a non-employment related capacity, such as when you are a consumer of a product or service offered by Assurant® in the open market, or when you are otherwise interacting with our websites or mobile applications unrelated to an interaction as a job applicant, or current or former employee, director, or independent contractor (hereafter referred to as "workforce member" or "you"). In those circumstances, the privacy notice posted or provided as part of the consumer product or service interaction shall apply.

Introduction

This Statement establishes guidelines that govern the collection, use and disclosure of the personal information of workforce members of Assurant.

"Personal information" means information about an identifiable workforce member, as more particularly defined or limited by applicable privacy laws.

Collecting, Using and Disclosing Personal Information

Assurant generally collects personal information from or concerning our workforce members as required or permitted by law, or for purposes related to establishing, maintaining, and concluding the employment or a similar relationship. For example, we may collect any of the following information about you:

Category of Personal Information We Collect	How We Use It
Identifiers and Contact information such as: Names, addresses, telephone numbers, mobile numbers, email addresses, dates of birth, marital status, next of kin or other family member or beneficiary information, Social Security numbers, driver's license or state identification numbers, photographs included on identification documents, bank account information, dependent and beneficiary information and other similar contact information and identifiers.	<ul style="list-style-type: none">• Collect and process employment applications, including confirming eligibility for employment, background and related checks, and onboarding• Process payroll and employee benefit plan and program administration including enrollment and claims handling• Maintain personnel records and record retention requirements• Communicate with employees and/or employees' emergency contacts and plan beneficiaries• Comply with applicable state and federal labor, employment, tax, benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws

	<ul style="list-style-type: none"> • Prevent unauthorized access to or use of Assurant property, including information systems, electronic devices, network, and data • Ensuring employee productivity and adherence to policies • Investigate complaints, grievances, and suspected violations of policy
<p>Sensitive Personal Information including protected class information under applicable law such as: Racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, commission, or alleged commission, of any crime, or as more particularly defined or limited by applicable law.</p>	<ul style="list-style-type: none"> • Comply with applicable state and federal employment laws • Design, implement, and promote our diversity, equity and inclusion programs • Carrying out services on your behalf, such as processing disability, dental and life insurance claims • Ensuring your health and safety in the workplace • Complying with non-discrimination requirements • In connection with actual or prospective legal proceedings • Considering reasonable adjustments to the workplace to accommodate you should you request an accommodation.
<p>Internet or other electronic network activity information such as: Activity on our information systems and communication systems (e.g.: internet browsing history activity, search history, intranet activity, email communications, social media postings, stored documents and emails, usernames, and passwords, phone calls, call logs, voice mails, text messages, chat logs, app use, and all other information regarding any systems and devices owned by Assurant®).</p>	<ul style="list-style-type: none"> • Facilitate the efficient and secure use of our information systems • Ensure compliance with information systems policies and procedures • Comply with applicable state and federal laws • Prevent unauthorized access to, use, or disclosure/removal of Assurant property, records, data, and information • Monitor or enhance employee productivity • Investigate complaints, grievances, and suspected violations of policy
<p>Geolocation data. This category includes GPS location data from Assurant-issued mobile devices and Assurant-owned vehicles.</p>	<ul style="list-style-type: none"> • Improve safety of employees who use Assurant property, equipment or services that allow geolocation tracking • Prevent unauthorized access, use, or loss of Assurant property • Investigate complaints, grievances, and suspected violations of policy
<p>Professional and employment-related information such as:</p>	<ul style="list-style-type: none"> • Recruiting • Collect and process employment applications, including confirming eligibility

<ul style="list-style-type: none"> • Data submitted with employment applications including employment history, employment recommendations, etc. • Information gathered from managers and others as part of performance evaluations and similar activities • Background check and criminal history • Work authorization • Professional licenses and educational degrees • Fitness for duty data and reports (upon return from a medical leave of absence) • Performance and disciplinary records • Salary and bonus data • Benefit plan enrollment, participation, and claims information • Charitable donations made through an Assurant program • Leave of absence information including religious and family obligations, physical and mental health data concerning employee and his or her family members 	<ul style="list-style-type: none"> • for employment, background and related checks, and onboarding • Employee benefit plan and program design and administration, including leave of absence administration • Performance evaluations • Maintaining personnel records and complying with record retention requirements • Communicating with employees and/or employees' emergency contacts and plan beneficiaries • Administration of Assurant's charitable giving programs • Complying with applicable state and federal labor, employment, tax, benefits, workers compensation, disability, equal employment opportunity, workplace safety, and related laws • Preventing unauthorized access to or use of Assurant's property, including information systems, electronic devices, network, and data • Ensuring employee productivity and adherence to policies • Investigating complaints, grievances, and suspected violations of policy
<p>Education information such as education history.</p>	<ul style="list-style-type: none"> • Evaluate an individual's appropriateness for hire or promotion.
<p>Inferences drawn from the PI in the categories above.</p>	<ul style="list-style-type: none"> • Engage in human capital analytics, including but not limited to, identifying certain correlations about individuals and success on their jobs, analyzing data to improve retention, and analyzing employee preferences to inform HR policies, programs, and procedures

Assurant collects and discloses personal information about workforce members from or to the workforce member himself or herself, and sometimes from or to third parties, including: Assurant affiliates; individuals providing references; third parties responding to authorized background checks; workplace monitoring mechanisms; third parties sending email, mail or other deliveries to workforce members; other employees completing performance appraisals, and colleagues providing comments with respect to a workforce member's performance; where appropriate, from medical professionals;

individuals conducting investigations in support of allegations of unlawful or inappropriate activity; and otherwise as required or permitted by law.

We may also disclose personal information to the following parties: to third parties for the purpose of providing references; to financial institutions for the purpose of confirming your salary and/or employment with your request or consent; to third parties connected with the contemplated or actual financing, insuring, sale, merger, transfer, or assignment of all or part of our business or assets; to regulatory or governmental authorities as requested or required for the purpose of fulfilling their mandates or responsibilities or to participate in grants and other related programs; to third parties connected with workplace safety/workers' compensation insurance plans for the purposes of managing and administering any claims or complaints; to third parties for emergency and disaster management purposes; to any other third party authorized by you; to any third party service providers you retain to facilitate or relocate, and to any other person as may be permitted or required by law.

Monitoring of Personal Information

To protect our customers, business, and workforce members, and to promote our compliance with applicable federal and local laws, Assurant may monitor your email, telephone calls, Internet usage, the movements of Assurant vehicles, as well as public areas with video surveillance. We may in the future monitor or may have already monitored for the purposes of:

- determining your compliance with Assurant policies and standards, such as the Assurant Privacy Policy and Assurant Code of Ethics;
- evaluating the quantity and quality of the work you produce;
- employing measures to protect the security of Assurant information and systems; and
- maintaining and promoting the safety and security of Assurant premises.

Please understand that you should have no expectation of privacy in email, mail, or other deliveries to Assurant.

Transfer of Personal Information

Assurant may also transfer your personal information, which may include sensitive information when needed to provide you services or to comply with applicable laws. This may be necessary for service providers hired to administer or provide products, services, or information on our behalf. We use reasonable measures to require that the organizations with which we share your personal information

for these purposes use your personal information only to perform the services we have hired them to provide. Some of the service providers that process or handle personal information on our behalf may be located outside of the country where you are employed. As a result, your personal information may be transferred, stored and/or processed outside the country where you are employed in connection with the purposes described in this Statement. We will only allow the transfer of your personal information to other countries that ensure an adequate level of protection for your personal information.

Security

Assurant will take reasonable precautions to protect personal information in its possession from loss, misuse and unauthorized access, disclosure, alteration, and destruction. Assurant protects data in many ways. Physical security is designed to prevent unauthorized access to database equipment and hard copies of sensitive personal information. Electronic security measures continuously monitor access to our servers and provide protection from hacking or other unauthorized access from remote locations. This protection includes the use of firewalls, restricted access, and encryption technology. Assurant limits access to personal information and data to those persons in Assurant's organization, or as agents of Assurant, that have a specific business purpose for maintaining and processing such personal information and data. Individuals who have been granted access to personal information are aware of their responsibilities to protect the security, confidentiality and integrity of that information and have been provided training and instruction on how to do so.

Your Consent

We collect, use, and disclose your personal information with your consent or as permitted or required by law. Your consent may be express or implied, depending on the circumstances and the sensitivity of the personal information in question. Your acceptance or continuation of employment with us will, in most cases, constitute consent for collections, uses and disclosures of certain personal information as described above. If you provide personal information about another person to us, we assume that you have the consent of that individual to enable us to collect, use or disclose his or her personal information (where applicable) as described in this Statement. If you provide personal information to Assurant, we assume that you consent to the collection, use and disclosure of your personal information as outlined in this Statement.

Although the collection, use and disclosure of your personal information is often required in an employment context, in some circumstances, such as when Assurant is offering you the opportunity to purchase goods or services unrelated to your employment, you may be permitted to refuse to consent to our collection, use and disclosure of your personal information or you may withdraw your consent to further collection, use and disclosure of information about you. In such cases, you should contact your local legal or Corporate Legal Department to determine whether legal and administrative requirements permit you to opt-out of the provision and use of this data.

Please note, however, in your capacity as a workforce member, Assurant does not sell or disclose personal information for money or other valuable consideration, and we do not share your personal information for cross context behavioral advertising, also known as targeted advertising. In addition, we do not use your personal information to evaluate, analyze or predict personal aspects related to your economic situation, health, preferences, interests, reliability, behavior, location or movements, or performance at work, which is also known as profiling, in furtherance of decisions that produce legal or similarly significant effects solely through an automated process that do not require final review and decision by a human.

We use Sensitive Personal Information only for the employment-related reasons described in this section.

Retention, Access, Correction and Complaints

We maintain a file, usually in electronic format, of your personal information for the above-mentioned purposes. This file is accessible by contacting your local People Organization Representative. Authorized Assurant employees, agents and mandataries have access to the file containing your personal information. Assurant retains your personal information for a period that a reasonable person would consider appropriate or as required or permitted by applicable laws.

You have the right to obtain access to any personal information about you that we hold, although our ability to provide you information may be limited in certain cases, such as where the burden or expense of providing access would be disproportionate to the risks to your privacy, or where the rights of persons other than you may be violated. If you wish to request access to, or correction of, your personal information in Assurant's custody or control, please make your request in writing to your local People

Organization Representative. In some circumstances, such as those specified above, or on matters relating to ongoing investigations relating to the security and integrity of Assurant and its operations, we may not provide you access to personal information, but we will do our best to minimize any such limitations.

If you believe that we maintain any information regarding you that is not accurate, please submit a letter of inquiry to your People Organization Representative. The People Organization Representative will promptly review your request for correction and will advise you either that the correction has been made, or alternatively, that Assurant has determined following reasonable review that the information is accurate, or that the matter continues to be under review. Should a review be taking place, you will be informed at the conclusion of the process of the outcome of the review, consistent with applicable law. If you have any other questions, requests, or complaints about our personal information practices, please submit your inquiry in writing to your People Organization Representative. Assurant will respond to any such questions or requests and will investigate any complaints to resolve them through a prompt, appropriate review and the results will be communicated to you.

Information Specific to Workforce Members in California

This section applies only to workforce members who are residents of California and is provided to comply with the California Consumer Privacy Act, as amended (“CCPA”).

Your Privacy Rights as a California Workforce Member

Unless an exemption under the CCPA or other applicable law applies, you may have the following rights:

- **Right to Know:** the right to request we disclose to you the following:
 1. Whether we are processing personal information about you;
 2. The categories of personal information we collected about you;
 3. The categories of sources from which we collected the personal information;
 4. The business or commercial purpose for collecting, sharing, and using personal information about you;
 5. The categories of third parties to whom we disclosed personal information about you; and
 6. The specific pieces of personal information we collected about you.
- **Right to Correct:** the right to request that we correct inaccurate personal information that we maintain about you.

- **Right to Delete:** the right to request that we delete personal information we, or an entity acting on our behalf, collected about you.

One or more of the rights described above may not be available if the personal information at issue is needed to:

- Comply with a legal obligation or Assurant's record retention schedule.
- Complete a transaction or otherwise perform a contract between you and Assurant.
- Detect, investigate, or prosecute against security incidents or malicious, fraudulent, or illegal activity.
- Identify and repair error to functionality of Assurant systems and assets.
- Enable uses internal to Assurant that are reasonable given your relationship with Assurant.
- Apply any additional exception permitted under the CCPA or other applicable law.

How to Exercise Your Privacy Rights if you are a California Workforce Member

You may exercise your privacy request rights by:

- Calling: 800-292-9155
- Completing the online form available www.assurant.com/dataprotection/caemployee

You will not be discriminated against, as defined at §1798.125 of the CCPA, for exercising these rights.

You must provide sufficient information that allows us to reasonably verify you are the person who is the subject of the rights request, or such person's authorized representative. We use a service provider to assist with identity verification and, as required or permitted by law, we may take steps to verify your identity prior to granting you access to information or acting on your request to exercise your rights. We may limit our response to your exercise of your rights as permitted under applicable law.

You may designate an authorized agent to request any of the above rights on your behalf. You may make such a designation by providing the agent with written permission, signed by you, to act on your behalf. If an agent makes a request on your behalf, as permitted by law, we may require verification of the agent's authorization to act on your behalf, require you to confirm you have authorized the agent to act on your behalf, or require you to verify your own identity. This may include, but is not limited to, a notarized financial/general power of attorney, court order, or official proof of guardianship.

Upon receiving your request, we will confirm receipt within ten (10) business days and respond to a verifiable consumer request within the timeframe required by relevant law.

If we are unable to honor your request, we will provide you with a written explanation of the reason(s). You have the right to contact us in writing if you wish to appeal our decision and we will provide you with a written response.

Assurant's record-keeping details as required under the CCPA are available here:

<https://www.Assurant.com/dataprotection/usa/ccpa-metrics>

Your Responsibilities

It is important to keep personal information accurate and up-to-date, particularly information required in order to process payroll and benefits. Please promptly report any change in personal information (address, phone number, family status, etc.) to the People Organization.

If you receive any complaint or inquiry in any way related to Assurant privacy practices or policies, please immediately direct that complaint to the People Organization.

Changes to this Statement

Assurant reserves the right to change this Statement at any time. You should review this Statement from time to time to ensure that you are aware of and accept any changes made.