

**Last Updated: February 5, 2024**

## **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 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 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 that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly with an identifiable workforce member, as more particularly defined or limited by applicable privacy laws.

## **Assistance for the Disabled**

Alternative formats of this Statement are available to individuals with a disability. Please contact [Accessibility@assurant.com](mailto:Accessibility@assurant.com) for assistance.

## **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
<p><b>Identifiers and Contact information</b> 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.</p>	<ul style="list-style-type: none"> <li>• Collect and process employment applications, including confirming eligibility for employment, background and related checks, and onboarding</li> <li>• Obtain motor vehicle records for individuals driving on Assurant business for the purpose of assessing driving risk.</li> <li>• Process payroll and employee benefit plan and program administration including enrollment and claims handling</li> <li>• Maintain personnel records and record retention requirements</li> <li>• Communicate with workforce members and/or employees’ emergency contacts and plan beneficiaries</li> <li>• Comply with applicable state and federal labor, employment, tax, benefits, workers’ compensation, disability, equal employment opportunity, workplace safety, and related laws</li> <li>• Prevent unauthorized access to or use of Assurant property, including information systems, electronic devices, network, and data</li> <li>• Ensuring workforce members productivity and adherence to policies</li> <li>• Investigate complaints, grievances, and suspected violations of policy</li> <li>• Facilitate certain clients’ assignment eligibility verification processes for workforce members who have access to client systems or information.</li> </ul>
<p><b>Sensitive Personal Information including protected classifications under applicable law</b> 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. Assurant collects personal information about membership in protected categories on a purely voluntary basis, except where required by law, and uses the information only in compliance with applicable laws and regulations.</p>	<ul style="list-style-type: none"> <li>• Comply with applicable state and federal employment laws or other legal obligations, including the reporting requirements of the federal Equal Employment Opportunity Act</li> <li>• Design, implement, and promote our diversity, equity and inclusion programs</li> <li>• Carrying out services on your behalf, such as processing disability, dental and life insurance claims</li> <li>• Ensuring your health and safety in the workplace</li> <li>• Complying with non-discrimination requirements</li> </ul>

	<ul style="list-style-type: none"> <li>• In connection with actual or prospective legal proceedings</li> <li>• Considering reasonable adjustments to the workplace to accommodate you should you request an accommodation.</li> </ul>
<p><b>Internet or electronic network activity, or other sensory/surveillance information</b> 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 / public profiles, 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"> <li>• Facilitate the efficient and secure use of our information systems</li> <li>• Ensure compliance with information systems policies and procedures</li> <li>• Comply with applicable state and federal laws</li> <li>• Identify potential candidates for employment opportunities</li> <li>• Prevent unauthorized access to, use, or disclosure/removal of Assurant property, records, data, and information</li> <li>• Monitor or enhance employee productivity</li> <li>• Investigate complaints, grievances, and suspected violations of policy</li> </ul>
<p><b>Geolocation data.</b> This category includes GPS location data from Assurant-issued mobile devices and Assurant-owned vehicles.</p>	<ul style="list-style-type: none"> <li>• Improve safety of employees who use Assurant property, equipment or services that allow geolocation tracking</li> <li>• Prevent unauthorized access, use, or loss of Assurant property</li> <li>• Investigate complaints, grievances, and suspected violations of policy</li> </ul>
<p><b>Professional and employment-related information</b> such as:</p> <ul style="list-style-type: none"> <li>• Data submitted with employment applications including employment history, employment recommendations, etc.</li> <li>• Information gathered from managers and others as part of performance evaluations and similar activities</li> <li>• Background check and criminal history</li> <li>• Work authorization</li> <li>• Professional licenses and educational degrees</li> <li>• Fitness for duty data and reports (upon return from a medical leave of absence)</li> <li>• Performance and disciplinary records</li> <li>• Salary and bonus data</li> <li>• Benefit plan enrollment, participation, and claims information</li> <li>• Charitable donations made through an Assurant program</li> <li>• Leave of absence information including religious and family obligations, physical and</li> </ul>	<ul style="list-style-type: none"> <li>• Recruiting</li> <li>• Collect and process employment applications, including confirming eligibility for employment, background and related checks, and onboarding</li> <li>• Employee benefit plan and program design and administration, including leave of absence administration</li> <li>• Performance evaluations</li> <li>• Maintaining personnel records and complying with record retention requirements</li> <li>• Communicating with workforce members and/or employees' emergency contacts and plan beneficiaries</li> <li>• Administration of Assurant's charitable giving programs</li> <li>• Complying with applicable state and federal labor, employment, tax, benefits, workers compensation, disability, equal employment opportunity, workplace safety, and related laws</li> </ul>

mental health data concerning employee and his or her family members	<ul style="list-style-type: none"> <li>• Preventing unauthorized access to or use of Assurant’s property, including information systems, electronic devices, network, and data</li> <li>• Ensuring workforce member productivity and adherence to policies</li> <li>• Investigating complaints, grievances, and suspected violations of policy</li> </ul>
<b>Education information</b> such as education history.	<ul style="list-style-type: none"> <li>• Evaluate an individual’s appropriateness for hire or promotion.</li> </ul>
<b>Biometric information</b> such as fingerprint, facial image recognition or retinal scan	<ul style="list-style-type: none"> <li>• To support facility access protocols at designated locations.</li> </ul>
<b>Inferences drawn from the PI in the categories above.</b>	<ul style="list-style-type: none"> <li>• 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</li> </ul>

Assurant collects personal information about workforce members from the workforce member himself or herself, vendors and service providers, as well as surveillance/recording technologies installed by Assurant, for example, video/CCTV surveillance in some common areas of Company facilities, and voicemail technologies, with consent to the extent required by law, and sometimes from third parties, including: Assurant affiliates; individuals providing references; third parties responding to authorized background checks or conducting motor vehicle record checks; public internet sources such as social media or public profiles; public records such as court records or records on file with other governmental or administrative agencies; 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 disclose personal information to the following parties: to service providers and contractors to assist us in meeting our business needs and contractual and legal obligations, to customers, for example, disclosing a service representative’s contact information to customers, 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 the purpose of underwriting Assurant's corporate auto insurance policy; 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 in Electronic Communications**

To protect our customers, business, and employees, and to promote our compliance with applicable federal and local laws, Assurant may monitor, access, and inspect your business and non-business email, voicemail, instant messages, and other communications and word processing documents, spreadsheets, and other files, stored on its electronic resources and/or on the systems of any third-party communications service provider under contract with Assurant (collectively, "Assurant Systems"), as well as telephone calls, Internet usage, the movements of Assurant vehicles, and public areas with video surveillance. As a result, communications, data, and files transmitted by, or stored on, Assurant Systems, including back-up copies, whether for business or non-business reasons, are not private or confidential vis-à-vis Assurant.

We may monitor 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.

At any times and by lawful means, Assurant may monitor any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage, of or through Assurant Systems. Assurant may conduct such monitoring by an electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems.

Assurant may, in its discretion, disclose any information stored on, or transmitted through, Assurant Systems to any third party, including law enforcement authorities or any other government agency. You may not use Assurant Systems to communicate with personal legal counsel. If you do so, Assurant will monitor these communications in the same manner in which it monitors other communications on the Assurant Systems, and you waive any privilege and expectation of privacy in these communications.

### **Transfer of Personal Information**

Assurant may also transfer your personal information, which may include sensitive information including but not limited to social security number, when needed to provide you employee benefits, to facilitate certain clients' assignment eligibility verification processes for workforce members who have access to client systems or information, or to comply with applicable laws. For example, such transfer of personal information may be necessary to service providers hired to administer or provide employee benefits or information on our behalf or to clients who require workforce members to be screened under the client's own protocols. We use reasonable measures to require that the organizations with which we disclose your personal information for these purposes use your personal information only to perform the services we have hired them to provide or for the other purposes contractually agreed upon. 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 or sensitive 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 automated processes 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**

We keep your personal information no longer than necessary for the purposes described above and in accordance with Assurant's Record Retention and Destruction Policy and Schedule unless Company is required to retain your personal information longer by applicable law or regulation, by administrative needs, by legal process, or to exercise or defend legal claims.

### **Information Specific to Workforce Members in California**

This section applies only to workforce members who are residents of California. For purposes of this California-specific section, the term workforce member also includes a job applicant.

#### California Notice at Collection

We collect the personal information identified in the chart above for the purposes identified in the corresponding chart column and retain it for the period described in Retention section below. We do not sell your personal information or disclose it for cross-context behavioral advertising. We also do not collect or process sensitive personal information for the purpose of inferring characteristics about you.

#### Your Privacy Rights as a California Workforce Member

Subject to applicable law, you may have the following rights:

- **Right to Know:** the right to request we disclose to you the following:
  1. The categories of personal information we collected about you;
  2. The categories of sources from which we collected the personal information;
  3. The business or commercial purpose for collecting, sharing, and using personal information about you;
  4. The categories of third parties to whom we disclosed personal information about you, and
  5. 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, taking into account the nature of the personal information and the purposes of processing the personal information
- **Right to Delete:** the right to request that we delete personal information that you have provided to the Company.

#### 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](http://www.assurant.com/dataprotection/caemployee)

You will not be discriminated against for exercising your rights under the California Privacy Rights Act.

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. To verify your identity, we match personal information that you provide us against personal information we maintain in our files. The more risk entailed by the request (e.g., a request for specific pieces of personal information), the more items of personal information we may request to reduce the risk that someone might try to impersonate you. If we cannot verify your identity to a sufficient level of certainty to respond to your request, we will let you know promptly and explain why we cannot verify your identity. 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.

### **Asia-Pacific Economic Cooperation Cross Border Privacy Rules**

The Assurant privacy practices, described in this Statement, comply with the Asia-Pacific Economic Cooperation Cross Border Privacy Rules System (APEC CBPR). The APEC CBPR system provides a framework for organizations to ensure protection of Personal Information transferred among participating APEC economies. More information about the APEC framework can be found [here](#).

### **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.

### **For More Information**

For questions or concerns about this Statement, please contact us at [MyHR@Assurant.com](mailto:MyHR@Assurant.com) or [theprivacyoffice@assurant.com](mailto:theprivacyoffice@assurant.com).