

Allianz Life Insurance Company of  
North America  
PO Box 59060  
Minneapolis, MN 55459-0060  
800.328.5600



## PRIVACY NOTICE

### APPLICANTS, EMPLOYEES, DIRECTORS, OFFICERS, AND CONTRACTORS

As a job applicant, employee, Director, Officer, or contractor, you have the right to know what categories of personal information Allianz Life Insurance Company of North America (Allianz) collects about you, how it is collected, and the purposes for which such information is collected.

As used in this Privacy Notice, “personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to you or your household. Personal information includes, but is not limited to, the categories of personal information identified below if such information identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular individual or household.

If you have any questions regarding this Privacy Notice or collection and use of your personal information by Allianz, please email us at [privacy@allianzlife.com](mailto:privacy@allianzlife.com). If you are a job applicant, employee, Director, Officer, or contractor who resides in California, this Privacy Notice is intended to comply with the California Consumer Privacy Act of 2018 (“CCPA”) as amended by the California Privacy Rights Act of 2020 (collectively “CCPA”). Additional details regarding our collection of personal information in non-employment-related contexts can be found on our website at [www.allianzlife.com](http://www.allianzlife.com) in our Online Privacy Policy, HIPAA Privacy Notice and Privacy Notice. If you have a disability that prevents or limits your ability to access this Privacy Notice, please contact us at 866.360.0603 or email us at [privacy@allianzlife.com](mailto:privacy@allianzlife.com). We will work with you to provide this Privacy Notice in an alternate format.

Allianz collects this information on behalf of itself and the following affiliates: Allianz Life Insurance Company of New York; AZOA Services Corporation; and Allianz Technology of America, Inc.; Allianz Global Investors; Allianz Capital Partners of America; Allianz Reinsurance of America; and AllianzGI US Holdings LLC.

This privacy notice is effective February 1, 2024.

### CATEGORIES OF PERSONAL INFORMATION WE COLLECT AND OUR BUSINESS PURPOSE FOR PROCESSING THAT INFORMATION

In each case as permitted by applicable law, we collect the following categories of personal information for the purposes described below. We provide additional information about our business purposes for processing your information below the chart. Inclusion of a category in the list below indicates only that we may collect this information about certain individuals for some activities within the scope of the business purpose identified. It does not necessarily mean that we collect all the information listed in a particular category for all employees, job applicants, Directors, Officers, or contractors.

We have shared information in each category with our affiliates and service providers for our business purposes within the last 12 months. As an insurance company, we may also receive requests for information from regulatory authorities,

our auditors, and/or our legal advisors. If requested from such parties, we would share your personal information as appropriate.

## APPLICANTS

### CATEGORIES OF PERSONAL INFORMATION COLLECTED FOR APPLICANTS

CATEGORY OF PERSONAL INFORMATION	TYPES OF APPLICANT INFORMATION COLLECTED
Personal Identifiers	Real name, alias, date of birth, postal address, telephone number, email address, unique personal identifier or online identifier, Social Security number, driver's license or state identification card number, passport number, written signature, or other similar identifiers.
Demographic Identifiers	Demographic information protected under federal law, California law, or other state law, including age, sex, gender, gender identity or expression, sexual orientation, national origin, citizenship, applicant's ability to work in the U.S. and whether sponsorship is required now or in the future, race, education level, and disability status or military/veteran status.
Employment Information	Employment history, professional licensures, professional or employment-related information, salary requirements, including written signatures and other information collected from a resume or application.
Education	Education history including educational institutions attended, degree(s) and/or certification(s) earned, and other academic information collected from a resume or application.
Internet or other Electronic Network Activity	Internet or other electronic network activity information, including online identifiers, internet protocol (IP) address, and information regarding an individual's or an individual's device interaction with an internet website.
Profile Information	Inferences drawn from any of the categories of information including creating a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
Audio/Visual Information	Audio, visual, or similar information including a recording of a customer service call, on-site cameras and video for security, an access badge photograph, and audio recordings.

### PURPOSES FOR WHICH WE MAY COLLECT AND SHARE PERSONAL INFORMATION

- To evaluate your application and consider a potential employment relationship with you.
- As needed to engage with you regarding your application, job opportunities, or a potential employment relationship with us, or to indicate authorization, acceptance, agreement, etc. to terms relating to an offer of employment.
- To verify your identity, perform background checks, verify past employment, educational history, professional standing, professional designations, certifications and qualifications.
- To comply with anti-discrimination laws and government reporting obligations, to help ensure equal employment opportunities.
- For internal reporting purposes including reporting and analytics to support diversity and inclusion programs.

- The technical administration, research, and development of the Allianz Career Website and the Recruiting system.
- To use digital identity insights to improve security.
- For quality assurance purposes, we collect audio recordings through recorded calls and company voice mail systems.
- To protect the physical security of our facilities via CCTV or by requiring badge identification.
- To assess your fitness and physical capacity for work.
- As otherwise required by applicable local, state, and federal laws.

In addition to the purposes identified above, Allianz may use and disclose personal information that we collect as necessary or appropriate to:

- Comply with laws and regulations, including, without limitation, applicable labor and employment, anti-discrimination, tax, health and safety, immigration, and social welfare laws.
- Detect, investigate, and protect against malicious, deceptive, fraudulent, or illegal activity.
- Monitor, investigate, and enforce compliance with and potential breaches of Allianz policies and procedures or legal and regulatory requirements.
- Comply with civil, criminal, judicial, or regulatory inquiries, investigations, subpoenas, or summons.
- Exercise or defend the legal rights of Allianz and its employees, Directors, Officers, affiliates, customers, contractors, and agents.

### SOURCES OF PERSONAL INFORMATION

- Directly from you and/or your device;
- Recruiters;
- Prior employers and professional references;
- Educational institutions;
- Pre-employment screening and background check services;
- Credentialing and licensing organizations;
- Publicly available sources, such as public social media profiles;
- Internal technology and security devices and software; and
- Other sources as directed by you.

### CATEGORIES OF SENSITIVE PERSONAL INFORMATION

We also collect the following categories of **sensitive personal information**. We generally use sensitive personal information only for the necessary purposes listed below.

CATEGORY OF SENSITIVE PERSONAL INFORMATION	TYPES OF SENSITIVE PERSONAL INFORMATION COLLECTED
Sensitive Personal Information / Not publicly available	Social Security number, driver’s license number, state identification card number, or race, ethnic origin, citizenship or immigration status, sexual orientation where you choose to disclose, and ability to perform job-related functions.

### PURPOSES FOR WHICH WE MAY COLLECT AND SHARE SENSITIVE PERSONAL INFORMATION

- To evaluate your application and consider a potential employment relationship with you.
- To verify your identity, perform background checks, verify past employment, educational history, professional designations, certifications and qualifications.

- To comply with anti-discrimination laws and government reporting obligations, to help ensure equal employment opportunities.
- For internal reporting purposes including reporting and analytics to support diversity and inclusion programs.
- As otherwise required by applicable local and federal laws.

**SOURCES OF SENSITIVE PERSONAL INFORMATION**

- Directly from you;
- Pre-employment screening and background check services;
- Educational institutions;
- Credentialing and licensing organizations; and
- Other sources as directed by you.

**EMPLOYEES, DIRECTORS, OFFICERS, AND CONTRACTORS  
(CURRENT AND FORMER)**

CATEGORY OF PERSONAL INFORMATION	TYPES OF INFORMATION COLLECTED
Personal Identifiers	Real name, alias, date of birth, postal address, telephone number, email address, unique personal identifier or online identifier, internet protocol (IP) address, Social Security number, driver’s license or state identification card number, passport number, signature, your citizenship, work permit status or other similar identifiers.
Demographic Identifiers	Demographic information protected under federal law, California law, or other state law, including age, sex, gender, gender identity or expression, sexual orientation, national origin, citizenship, race, education level, marital status, health and disability status or military/veteran status.
Employment Information	Employment history, professional licensures, professional or employment-related information, salary information, including written signatures and other information collected from a resume or application.
Education	Education history including educational institutions attended, degree(s) and/or certification(s) earned, and other information collected from a resume or application or that you may submit during your engagement with Allianz.
Financial Information	Bank account information
Medical Information	Health insurance information, including an individual’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in the individual’s application and claims history. Medical information, including any information in possession of or derived from a healthcare provider, healthcare service plan, pharmaceutical company, or contractor regarding an individual’s medical history, medical condition (mental or physical), or treatment.
Internet or Other Electronic Network Activity	Internet or other electronic network activity information, including online identifiers, and information regarding an individual’s or an individual’s device interaction with an internet website. Network Activity Data such as internet or other electronic network activity information, which may include browsing history or search history.
Profile Information	Inferences drawn from any of the information listed above, including creating a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Audio/Visual Information	Audio, visual, or similar information including a recording of a customer service call, on-site cameras and video for security, an access badge photograph, and audio recordings.
--------------------------	---

**PURPOSES FOR WHICH WE MAY COLLECT AND SHARE PERSONAL INFORMATION**

- To manage your employment or contractor relationship with us or manage your appointment as a director or an officer.
- For compensation, payroll, tax, benefits eligibility, enrollment, and administration.
- For workforce and performance management, including personnel planning, productivity monitoring, and evaluation.
- For workforce development, education, training, and certification.
- To authenticate your identity and verify your access permissions to provide access to Allianz systems, networks, databases, equipment, and facilities.
- To implement, monitor, maintain, and secure Allianz systems, networks, databases, applications, equipment, and facilities.
- To arrange, confirm, and monitor work-related travel, events, meetings, and other activities.
- To contact and communicate with you regarding your employment, job performance, compensation, and benefits, or in the event of a natural disaster or other emergency.
- To contact and communicate with your designated emergency contacts in the event of an emergency, illness, or absence.
- To contact and communicate with your dependents and designated beneficiaries in the event of an emergency or in connection with your benefits.
- To provide you with employee rewards and recognition such as (cards, gifts, snack boxes, etc.)
- For purposes such as workplace accommodations, benefits administration assistance, or similar purposes.
- To assess your working capacity or the diagnosis, treatment, or care of a condition impacting your fitness for work, and other preventive or occupational medicine purposes (including work-related injury and illness reporting).
- To deduct premiums from your paycheck, Allianz will receive limited information about your enrollment if you participate in company plans.

In addition to the purposes identified above, Allianz may use and disclose personal information that we collect as necessary or appropriate to:

- Comply with laws and regulations, including, without limitation, applicable labor and employment, anti-discrimination, tax, health and safety, immigration, and social welfare laws.
- Detect, investigate, and protect against malicious, deceptive, fraudulent, or illegal activity.
- Monitor, investigate, and enforce compliance with and potential breaches of Allianz policies and procedures or legal and regulatory requirements.
- Comply with civil, criminal, judicial, or regulatory inquiries, investigations, subpoenas, or summons.
- Exercise or defend the legal rights of Allianz and its employees, Directors, Officers, affiliates, customers, contractors, and agents.

**SOURCES OF PERSONAL INFORMATION**

- Directly from you and/or your device;
- Recruiters;
- Prior employers and professional references;
- Educational institutions;
- Pre-employment screening and background check services;
- Credentialing and licensing organizations;

- Insurance providers, including health, disability, and life insurance;
- Publicly available sources, such as public social media profiles;
- Internal technology and security devices and software; and
- Other sources as directed by you.

**CATEGORIES OF SENSITIVE PERSONAL INFORMATION**

We also collect the following categories of **sensitive personal information**. We generally use sensitive personal information only for the necessary purposes listed below.

CATEGORY OF SENSITIVE PERSONAL INFORMATION	TYPES OF SENSITIVE PERSONAL INFORMATION COLLECTED
Sensitive Personal Information / Not publicly available	Social Security number, driver’s license number, state identification card number, or passport number, race, ethnic origin, citizenship or immigration status, sexual orientation, gender identity, and pronouns where you choose to disclose, health, physical characteristics or description, and ability to perform job-related functions.

**PURPOSES FOR WHICH WE MAY COLLECT AND SHARE SENSITIVE PERSONAL INFORMATION**

- To manage your employment or contractor relationship with us or manage your appointment as a director or an officer.
- For compensation, payroll, tax, benefits eligibility, enrollment, and administration.
- To authenticate your identity.
- For purposes such as workplace accommodations, benefits administration assistance, and similar purposes.
- To assess your working capacity or the diagnosis, treatment, or care of a condition impacting your fitness for work, and other preventative or occupational medicine purposes (including work-related injury and illness reporting).
- To deduct premiums from your paycheck, Allianz will receive limited information about your enrollment if you participate in company plans.
- To comply with anti-discrimination laws and government reporting obligations, to help ensure equal employment opportunities.
- For internal reporting purposes including reporting and analytics to support diversity and inclusion programs.
- As otherwise required by applicable local and federal laws.

**SOURCES OF SENSITIVE PERSONAL INFORMATION**

- Directly from you;
- Educational institutions;
- Pre-employment screening and background check services;
- Credentialing and licensing organizations;
- Insurance providers, including health, disability, workers’ compensation, and life insurance; and
- Other sources as directed by you.

You can find additional details about our collection of personal information in our Online Privacy Policy, HIPAA Privacy Notice and Privacy Notice.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

## DISCLOSURE OF PERSONAL INFORMATION

We may disclose your personal information to third parties (e.g., service providers) for business purposes. When we disclose personal information for a business purpose, we enter into a contract that describes that purpose and requires the recipient to keep the personal information confidential, and not to use it for any purpose other than performing the contract. We may transfer your information to another country for processing as permitted and in compliance with applicable law. We do not sell your personal information to third parties, and we do not share your information for cross-context behavioral advertising purposes, as defined under California law. We may share your personal information for the business purposes described in this California Applicant, Employee, Director, Officer, Director Privacy Notice with the following parties:

CATEGORY	DESCRIPTION
Corporate Affiliates	We may share your information with our corporate affiliates and with their respective officers, directors, employees, accountants, attorneys, and agents.
Acquisitions and Similar Transactions	If the company is sold or part of its assets are merged with another company, your personal data may be transferred as part of the merger or sale.
Disclosures with Your Consent	We may ask if you would like us to share your information with other unaffiliated third parties not described elsewhere in this Policy. We will only disclose your information in this context with your consent.
Legal Obligations and Rights (Subpoenas, Court Orders, and Warrants); Regulatory Authorities	We may disclose information to comply with the law, including disclosure to relevant industry regulatory bodies, or in response to subpoenas, warrants, court orders, or other legal process.
Service Providers	We may share your personal information with service providers, such as recruiters, pre-employment screening services, third-party benefits administrators, payroll processors, background check providers, and others.
Professional Advisors (Auditors and Legal Advisors)	We may share your information with our professional advisors, including attorneys, auditors, and accountants, to provide services on our behalf.
De-identified or Aggregated Data	We may disclose aggregated information or de-identified information about our users that does not identify any specific individual.
Other	Where permitted by law.

## PERSONAL DATA STORAGE AND RETENTION

We and our service providers store personal information on computer systems. We keep records containing personal information in accordance with applicable state and federal regulations or contractual obligations. We aim to retain personal information only for as long as necessary for the purposes it was collected for, including defending or advancing legal claims, and to comply with legal obligations. We may need to keep some personal information for longer than other information to comply with applicable laws and regulations, including litigation.

When determining how long to retain a record, including any personal information it contains, we consider the following criteria:

- The length of time the record is needed to provide the products and services you request and maintain our business relationship.
- The length of time the record is needed to support and improve our operational processes.

- The length of time the record is needed to protect our rights and legal interests.
- The length of time the record must be kept to comply with applicable laws and regulations.

The same personal information about you may be included in more than one record and used for more than one purpose, each of which may be subject to different retention periods based on the factors listed above.

We may delete personal information if we believe it is incomplete, inaccurate, or that our continued storage of it is contrary to our objectives or legal obligations. When we delete data, we remove it from our active servers and databases, but it may remain in our archives when it is not practical or possible to delete it.

To the extent permitted by law, we may retain and use anonymous, de-identified, or aggregated information for performance reporting, benchmarking, and analytic purposes and for product and service improvement.

## YOUR PRIVACY RIGHTS

If you are a California resident, California law provides you with specific rights regarding your personal information, subject to certain limitations. This section describes these rights and explains how to exercise those rights if they apply to you.

- 1. Right to Access Your Data.** You have the right to request that we disclose certain information to you about our collection and use of your personal information. Once we receive and confirm your verifiable request, you have the right to receive:
  - The categories of personal information we collected about you.
  - The categories of sources for the personal information we collected about you.
  - Our business or commercial purpose for collecting, selling or sharing that personal information.
  - The specific pieces of personal information we collected about you, including or by a service provider or contractor.
  - The categories of third parties with whom we share that personal information.
  - The specific pieces of personal information we have disclosed for a business or commercial purpose, identifying the personal information categories that each category of recipient obtained about you.

Any disclosures we provide will only cover the 12-month period preceding the receipt of your request. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

- 2. Right to Data Portability.** You have the right to a “portable” copy of your personal information that you have submitted to us. Generally, this means you have a right to request that we move, copy or transmit your personal information stored on our servers / IT environment to another service provider’s servers / IT environment.
- 3. Right to Correction.** You have the right to request correction or changes to your personal information if it is inaccurate or out of date.
- 4. Right to Delete Your Data.** You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.
- 5. Right to Opt Out of Sale or Sharing of Personal Information.** We currently do not sell personal information to third parties or share personal information about job applicants, employees, Directors, Officers, or contractors with third parties for cross-context behavioral advertising purposes, and therefore do not offer this option. We may disclose personal information about you to our affiliates and service providers as permitted by law. Please see the “Sharing Personal Information” portion of this policy for more information.



6. **Right to Limit Use and Disclosure of Sensitive Personal Information.** You have the right to request we limit the use of your sensitive personal information to only purposes necessary to engage with you as a job applicant, employee, Director, Officer, or contractor. California law defines this sensitive personal information, and you can find a more detailed description of the types of information in the charts included above. We only use your sensitive personal information for necessary purposes, such as engaging with you as an employee, job applicant, Director, Officer, or contractor, protecting and securing your personal information and our systems, verifying or maintaining the quality or safety of our services and systems, or as allowed by regulations or required by law.
7. **Right to Non-Discrimination.** We will not discriminate against you for exercising any of your privacy rights.

## **EXERCISING YOUR RIGHTS**

To exercise your rights described above, please submit a verifiable request using one of the methods listed below:

- Calling us at 800.328.5600
- Contacting us through the secured website [www.allianzlife.com](http://www.allianzlife.com)
- Writing to us at:  
Allianz Life Insurance Company of North America  
Attn: Privacy Office  
PO Box 59060  
Minneapolis, MN 55459-0060

### ***Verification***

For some personal information requests, we may need to verify your identity before fulfilling your request. To verify your identity, we will collect information from you, including, to the extent applicable, your name, government identification number, date of birth, contact information, your account information, answers to security questions, or other personal identifying information. We will match this information against information we have previously collected about you or against information available from consumer reports to verify your identity and to respond to your request. We will only use the information collected to verify your request and respond to your personal information request. If we are unable to verify your identity as part of your request, we will not be able to satisfy your request. For deletion requests, you will be required to submit a verifiable request for deletion and then to confirm separately that you want personal information about you deleted.

### ***Authorized Agent***

Only you, or someone legally authorized to act on your behalf, may make a verifiable request related to your personal information. If you would like to appoint an authorized agent to make a request on your behalf, you must provide the agent with written, signed permission to submit privacy right requests, on your behalf, or provide a letter from your attorney. The agent or attorney must provide this authorization at the time of the request. We may require you to verify your identity with us directly before we provide any requested information to your approved agent.

### ***Response Timing and Format***

If you are entitled to any of the above-described rights, we endeavor to respond to a verifiable request within forty-five (45) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing.

We will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will cover the 12-month period preceding receipt of a verifiable request; however, you may have the right to request access to personal information that is more than 12 months old. The response we provide will

also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

## **CHANGES TO OUR PRIVACY NOTICE**

We reserve the right to amend this Privacy Notice at our discretion and at any time.

## **CONTACT INFORMATION**

If you have any questions or comments about this notice, the ways in which we collect and use your information described here, your choices and rights regarding such use, or wish to exercise your rights under California law, please contact us by:

- Calling us at 800.328.5600
- Emailing us via [privacy@allianzlife.com](mailto:privacy@allianzlife.com)
- Contacting us through the secured website [www.allianzlife.com](http://www.allianzlife.com)
- Writing to us at:  
Allianz Life Insurance Company of North America  
Attn: Privacy Office  
PO Box 59060  
Minneapolis, MN 55459-0060