ASPIRIANT

# Protecting Your Personal Information

## Privacy Rights and Policies

Financial companies, such as Aspiriant, choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal and state law also requires us to tell you how we collect, manage, use, share and protect your personal information. Please read this notice carefully to understand Aspiriant's practices.

We respect your privacy and are committed to protecting it though our compliance with this policy. In this notice, we describe the types of information we may collect from you and our practices for collecting, managing, using, protecting and disclosing that information.
This policy applies to information we collect:

- On our website
- By email, text and/or other electronic messages
- When you interact with our advertising and software applications on third-party websites and access the related services
- During our meetings, events and conferences, either in person, over video chat or via webinar
- From any third-party service provider that may share information with us in order to provide services to you

### Who does this policy apply to?

Aspiriant collects information from or regarding clients, prospective clients ("prospects"), employees and candidates for employment ("candidates"). This policy applies to the personal information of all these categories of people.

### What are the categories of personal information we collect?

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly ("personal information"), with you or your household ("consumer").

Personal information does not include publicly available information from government records, de-identified or aggregated consumer information or records that we have a reasonable basis to believe is lawfully made available to the general public by you.

### What is Sensitive Personal Information?

Sensitive Personal Information ("SPI") is a special subset of personal information, including:

- Social Security, driver's license, state identification card, or passport number
- Account login, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account
- Precise geolocation
- Racial or ethnic origin, religious or philosophical beliefs, or union membership
- Mail, email, and text message content, unless the business is the intended recipient of the communication

- Genetic data
- Personal information collected and analyzed concerning a consumer's" health, sex life or sexual orientation is also considered sensitive personal information

As described below, we apply further protections to SPI.

## What information do we collect, how do we collect it, and why?

The three tables below provide details about the categories of personal information we've collected from clients, prospects, employees, and candidates within the last 12 months. We've organized the tables as follows:

1. Applies to clients, prospects, employees and candidates
2. Applies to clients and prospects only
3. Applies to employees and candidates only

We do not rent or sell your personal information or SPI to anyone.

| This section applies to clients, prospects, employees and candidates: | | | | | |
|---|---|---|---|---|---|
| Category | Examples of Personal Information | Collected by Us? | Disclosed by Us? | Source of Information* | Business Purpose* |
| Identifiers | A real name, alias, postal address, unique personal identifier, Internet protocol address, email address, account address, Social Security number, driver's license number, passport number, or other identifiers | Yes | Yes | 1, 2, 3, 4 | A, B, C, D, E,F |
| Personal information | A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information | Yes | Yes | 1, 2, 3, 4 | A, B, C, D, E |

| This section applies to clients, prospects, employees and candidates: | | | | | |
|---|---|---|---|---|---|
| Category | Examples of Personal Information | Collected by Us? | Disclosed by Us? | Source of Information* | Business Purpose* |
| Protected classification characteristics under state or federal law | Age (40 years or older, qualifies as protected), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status | Yes | Yes | 1, 2, 3, 4 | A, B, C, D, E |
| Internet or other similar network activity | Browsing history, search history, information on a consumer's interaction with a website, application or advertisement | Yes | Yes | 3 | B, C, D, E |
| Inferences drawn from other personal information | Profile reflecting a person's preferences, characteristics, trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes | Yes | Yes | 1, 3 | A, B, C |
| Sensory Data | Audio, electronic, visual, thermal, olfactory or similar information | Yes | Yes | 1, 2, 3 | A, B, C, D |
| Professional or employment-related information | Current or past job history or performance evaluations | Yes | Yes | 1, 2, 3, 4 | A, B, C, D, E, F |
| Non-public education information | Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student ID codes, student financial information, or student disciplinary records | Yes | Yes | 1, 4 | A, D, E |

*Please see descriptions further below for sources of personal information and how we use that personal information for business purposes

| This section applies to clients and prospects only: | | | | | |
|---|---|---|---|---|---|
| Category | Examples of Personal Information | Collected by Us? | Disclosed by Us? | Source of Information* | Business Purpose* |
| Commercial information | Records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies | Yes | Yes | 1, 2, 4 | A, B, C, D, E |

| This section applies to employees and candidates only: | | | | | |
|---|---|---|---|---|---|
| Category | Examples of Personal Information | Collected by Us? | Disclosed by Us? | Source of Information* | Business Purpose* |
| Biometric Information | Genetic, physiological, behavioral and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, voice prints, iris or retina scans, keystroke, gait or other physical patterns, and sleep health or exercise data | Yes | Yes | 1, 4 | A, C, D, E |
| Geological data | Physical location or movements | Yes | Yes | 1, 4 | C |

*Please see descriptions further below for sources of personal information and how we use that personal information for business purposes

## Where do we obtain personal information about you ("Source of Information")?

We obtain the categories of personal information listed above from the following categories of sources:

1. Directly from you or your agents. For example, from documents that you provide to us to render services to you and copies of your correspondence, including your email address or information an employee may provide for benefits purposes.

2. Indirectly from you or your agents. For example, information we receive from your other service providers such as accountants, lawyers and other financial institutions.

3. Directly and indirectly from activity on our websites. For example, from submissions through our website portal or website usage details collected automatically or information we collect through cookies and automatic data collection technologies as you navigate though and interact with our website.

4. From third parties that interact with us in connection with services we perform or provide data to us with your authorization. For example, from custodians when they service your brokerage accounts.

## How do we use your personal information in our business ("Business Purpose")?

We may collect or use the personal information we collect for one or more of the following business purposes:

A. To fulfill or meet the reason you provided the information. For example, to fulfill the terms of your Engagement Agreement with us or complete your request for proposal, assess your application for employment, or provide employee benefits.

B. To provide you with support and respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.

C. To respond to law enforcement requests and as required by applicable law, court order or governmental regulations, or in the event that we have reason to believe someone is causing or threatening to cause injury to, or interfere with, our or your rights or property.

D. As described by you when collecting your personal information or as otherwise set forth in applicable state and federal law.

E. In connection with a corporate reorganization, merger, joint venture, sale, transfer or other disposition of all or any portion of our business or shares or in connection with bankruptcy, or some other change of control. Personal Information could be one of the assets transferred to or acquired by a third party.

F. Commercial Purposes to market Aspiriant's services to you or another person

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

## How and when do we share your personal information, as defined by the Securities and Exchange Commission's Regulation S-P?

All financial companies need to share clients' personal information to run their everyday business. When we disclose personal information for a business purpose, we generally enter into a contract that describes the purpose and requires the recipient to keep your personal information confidential and not use it for any purpose other than for the purpose provided. In the section below, we list the reasons we can share your personal information, the reasons we choose to share your personal information, and whether you can limit this sharing.

| Reasons we may share your personal information | Does Aspiriant, LLC share? | Can you limit this sharing? |
|---|---|---|
| For our everyday business purposes — Such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus | Yes | No |
| For marketing purposes — Such as offers of our products and services to you | Yes | Yes |
| For joint marketing with other financial companies | No | Do Not Share |
| For our affiliates' everyday business purposes — Such as information about your transactions and experiences | Yes | No |
| For our affiliates' everyday business purposes — Such as information about your creditworthiness | No | Do Not Share |
| For our affiliates to market to you | No | Do Not Share |
| For nonaffiliates to market to you | No | Do Not Share |

## Who do we share information with?

As an RIA, we primarily share your information with:

- Custodians
- Fund Administrators/ Managers
- Technology and service providers
- Regulators (when required)

## How do we protect your information?

To protect your personal information from unauthorized access and use, we implement safeguards in accordance with Regulation S-P, including:

- Administrative controls (policies, employee training, vendor oversight)
- Technical safeguards (encryption, MFA, access controls, monitoring)
- Physical safeguards (secure office access and document controls)

We also maintain an incident response program designed to detect, contain, respond to and notify affected individuals of unauthorized access to their sensitive personal information as required by SEC rules.

## Incident Notification

If your sensitive personal information is accessed or used without authorization, we will provide notice as soon as practicable, consistent with SEC Regulation S-P requirements.

## Why can't I limit all sharing?

Federal and state law gives you the right to limit only certain types of sharing. State laws provide additional rights described below.

## What are your rights and choices?

Federal and laws of various states provide you with specific rights regarding your personal information. We provide these rights to our clients regardless of the state in which they reside. This section describes your rights and how to exercise those rights.

**Access to specific information and data portability rights**

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the previous 12 months. Once we receive and verify your request, we will disclose to you:

- 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 or selling that personal information
- The categories of third parties with whom we share that personal information
- The specific pieces of personal information we collected about you (also called a data portability request)
- If we disclosed your personal information for a business purpose, the personal information categories that each category of recipient obtained

**Right to limit use and disclosure of sensitive personal information**

You have the right to request limitation of use and disclosure of your SPI that we collect from you or about you and retain. Once we have received and verified your limit request, we will limit use and disclosure unless an exception applies as outlined below.

We may deny your limitation request if the use and/or disclosure of the information is necessary for us or our service providers to:

- Complete the transaction for which we collected the personal information, provide a service that

you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you
- Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for such activities
- Debug products to identify and repair errors that impair existing intended functionality
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provide for by law
- Comply with Graham Leach Bliley Act (GLBA) also known as the Financial Modernization Act of 1999, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Confidentiality of Medical Information Act (CMIA), and California Financial Information Privacy Act (FIPA)
- Fulfill a solely internal purpose reasonably aligned with consumer expectations based on your relationship with us
- Comply with regulatory record retention or other legal requirements
- Make other internal or lawful uses of that information that are compatible with the context in which you provide it

**Correction request rights**

You have the right to request correction of any incorrect personal or sensitive personal information that we collected from you or about you and retain. Once we receive and verify your request, we will make the corrections (and direct our service providers to correct) to your personal information.

**Deletion request rights**

You have the right to request that we delete any of the personal information that we collected from you or about you and retained, subject to certain important exceptions. Once we receive and verify your request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies as outlined below.

We may deny your deletion request if retaining the information is necessary for us or our service providers to:

- Complete the transaction for which we collected the personal information, provide a service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you
- Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for such activities
- Debug products to identify and repair errors that impair existing intended functionality
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provide for by law
- Comply with Graham Leach Bliley Act (GLBA) also known as the Financial Modernization Act of 1999, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Confidentiality of Medical Information Act (CMIA), and California Financial Information Privacy Act (FIPA)
- Fulfill a solely internal purpose reasonably aligned with consumer expectations based on your relationship with us
- Comply with regulatory record retention or other legal requirements
- Make other internal or lawful uses of that information that are compatible with the context in which you provide it

**Exercising access, data portability, correction, and deletion rights**

To exercise the access, data portability, correction, and deletion rights described above, please submit a request to us by either:

- Call us at 1.866.394.0394
- Visiting Aspiriant.com (https://www.aspiriant.com)

Note that all such requests must be a "verifiable consumer request" in accordance with the law. Only you or a duly authorized person acting on your behalf, may make a request related to personal

information. You may also make a request on behalf of your minor child. A "duly authorized person" to act on your behalf is your attorney-in-fact, someone holding a general power of attorney, or a person registered with an applicable state authority.

You may only make a request for access or data portability twice within a 12-month period. The request must:

- Provide enough information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative
- Describe your request with enough detail that allows us to properly understand, evaluate and respond to it

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. We will only use personal information provided in a request to verify the requestor's identity or authority to make the request.

**Response timing and format**

We endeavor to respond to a consumer's request within 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 only cover the 12-month period preceding the request's receipt. 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 that should allow you to transfer the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your 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 we process your request.

If you are a new client, we can begin sharing your information 10 days from the date we sent this notice. When you are no longer our client, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.

## Data Retention

We retain personal information as long as necessary to:

- Provide services to clients
- Comply with SEC and other legal obligations

## Changes to our Privacy Notice

We reserve the right to amend this Privacy Rights and Policies notice at our discretion and at any time. When we make changes to this Privacy Rights and Policies notice, we will notify you by email or through a notice on our website homepage.

## Contact Information

If you have any questions or comments about this Privacy Rights and Policies notice, the ways in which we collect or use your personal information, or your choices and rights regarding such use, or if you wish to exercise your rights under federal or state law, please do not hesitate to contact us at:

Phone: 1.866.394.0394
Website: aspiriant.com
Email: compliance@aspiriant.com