Growsin — Privacy Policy & Compliance Framework

(SEBI, DPDP Act & IT Act Compliant)

Part 1: Introduction

I, operating as Growsin, am committed to protecting the confidentiality and privacy of every client who entrusts me with their personal and financial information. This Privacy Policy explains in detail how I collect, process, use, store, retain, and protect client data while providing investment advisory and research services in compliance with the Securities and Exchange Board of India (SEBI) regulations, the Digital Personal Data Protection Act, 2023 (DPDP Act), and the Information Technology Act, 2000 including the Sensitive Personal Data or Information (SPDI) Rules, 2011.

My role as an adviser is not merely transactional; it is fiduciary in nature. This means that I am bound by law and by principle to always place the client's interests above my own. Confidentiality of information is central to this fiduciary duty. The trust that clients place in me extends beyond the quality of investment advice or research; it extends equally to the expectation that their personal and financial information will never be misused, exposed, or shared improperly.

Unlike large firms with complex hierarchies, Growsin operates as an individual advisory practice. This means that only I, personally, access and process client data.

No one else is involved in data handling. If, at any time in the future, I engage support staff or external service providers, they will be strictly bound by confidentiality and by the same standards of protection described in this Policy. The simplicity of this structure enhances security because access points are minimized, and responsibility rests solely with me.

This Policy is intended for all categories of clients - whether retail investors, high- net-worth individuals, ultra-high-net-worth individuals, or non-resident Indians - who engage with me for advisory or research services. It applies across all channels of communication, whether you share information through email, phone calls, video consultations, digital client portals, or in-person interactions. The commitment to confidentiality and lawful use of information is the same regardless of the medium.

I am legally required to retain certain records for a minimum of five years as per SEBI regulations. This includes client agreements, KYC documents, risk profiling forms, investment advice, and communications. Once the legally required retention period ends, and unless another law requires longer storage, I delete or securely anonymize the information. This practice ensures that client information is not kept indefinitely and is always aligned with the principle of purpose limitation under the DPDP Act.

I may work with vendors such as hosting providers, payment gateways, and cloud storage services to deliver services efficiently. These vendors are permitted to handle client information only for the specific purpose for which they are engaged, and they are required to maintain confidentiality and implement reasonable safeguards. No vendor has the right to use client data for its own purposes, and I remain accountable for ensuring that client information is protected even when handled by third parties.

It is important for clients to know that their data may be disclosed to regulators such as SEBI, the Financial Intelligence Unit (FIU-IND), or the Income Tax Department when required by law. Similarly, disclosure may occur if directed by a court of law or other lawful authority. These disclosures are limited to what is strictly required by the regulator or court order. I do not sell, lease, or otherwise disclose client information for marketing or unrelated commercial purposes.

This Policy also outlines the rights that clients have under the DPDP Act, such as the right to access their data, request corrections, ask for erasure once retention

obligations expire, withdraw consent for optional services, and raise grievances. These rights are recognized and respected in both letter and spirit. I handle all such requests personally and respond within the timelines set out in this Policy.

By engaging with Growsin, you consent to the practices described in this Privacy Policy. This Policy forms part of the terms of engagement between me and my clients. It reflects not only legal compliance but also my professional philosophy that trust and confidentiality are inseparable from investment advisory and research services.

The sections that follow explain, in greater detail, the scope of this Policy, the legal framework governing data protection, the categories of data I collect, the lawful basis for processing it, the purposes for which it is used, retention rules, disclosures, safeguards, client rights, and how you may reach me with questions or concerns.

Each section has been written with clarity and transparency in mind so that clients can feel reassured about how their information is handled from the moment it is collected until the day it is lawfully deleted.

Part 2: Scope and Applicability

This Privacy Policy applies to every client who engages with me through Growsin for investment advisory or research services. It is designed to provide complete clarity about how personal and financial data is handled from the moment you first interact with me, whether that is through my website, by email, over the phone, or during an in-person consultation. It does not matter whether you are an individual investor just

beginning your journey, a high-net-worth individual with complex portfolios, or a non-resident Indian managing assets across borders. The commitments I make in this Policy apply equally to all clients without exception.

The scope of this Policy is intentionally broad because in today's environment, data does not flow through a single channel. A client may send me a scanned KYC document by email, may speak with me on the phone about risk appetite, may share financial details in a digital form through a secure client portal, or may provide information verbally during a consultation. This Policy ensures that all of these interactions - digital or physical, direct or through approved third-party vendors - are covered by a consistent set of rules and obligations.

It is also important to clarify what this Policy does not cover. There are certain platforms and channels where data may be exchanged but which are not under my direct control. For example, if a client accesses their demat account through a broker's portal, or if they interact with me casually through a social media platform like WhatsApp, Twitter, or LinkedIn, the privacy of those interactions is primarily governed by the policies of those platforms. While I make every effort to ensure that sensitive matters are discussed only through secure and approved channels, clients should remain mindful of the limitations of third-party applications. That said, if information from such channels is brought into my advisory process, it immediately becomes subject to the protections of this Policy.

Since Growsin operates as an individual advisory practice, only I access and process client information. No one else - no employees, no associates, no IT teams - has access to the data you provide. If I ever decide to engage support staff in the future to help with administrative or operational work, those individuals will be strictly bound by confidentiality agreements and will be permitted to handle data only to the minimum extent necessary to perform their duties. Until such a time, the responsibility and control remain entirely with me. This structure keeps data flows simple and enhances accountability because there is never any doubt about who is responsible.

I may rely on vendors to facilitate certain services. These include hosting providers who run the servers that support my website or client portal, payment gateways that process service fees or refunds, and cloud storage providers who may hold encrypted copies of records. Such vendors are included within the scope of this Policy because they may handle client data as part of their operations. However, their

role is limited: they are permitted to use the data only as required to provide their services, and they must maintain confidentiality and follow reasonable security practices. I ensure that these vendors cannot access or use client data for any purpose beyond what is necessary.

The scope of this Policy also extends to the different categories of data that I may collect. Personal data includes basic identifiers like your name, address, and contact details. Financial data includes income, investments, liabilities, and other relevant details needed to provide tailored advice. Sensitive personal data, such as bank account information or authentication details, is also covered. Technical data such as IP addresses or device identifiers, while less personal, is included because it may help protect against fraud. Communication records, such as emails, phone logs, and advisory notes, are likewise included because they form part of the regulated advisory process under SEBI rules.

This Policy is not limited to any specific form of record. Whether your data exists as a paper document stored securely in physical form or as a digital record maintained in an encrypted server, the obligations described here apply equally. The format of storage does not change the standard of care. I apply the same diligence to securing a physical copy of your PAN card as I do to encrypting a digital file containing your financial plan.

Finally, the scope of this Policy includes the full life cycle of data. It begins at the point of collection, continues through the various stages of processing and use, and extends until lawful deletion or anonymization. The Policy also governs what happens in exceptional situations such as disclosures to regulators or responses to data breaches. By covering every stage of the data life cycle, I aim to provide clients with a holistic and consistent framework for understanding how their information is handled.

In summary, the applicability of this Policy is straightforward: if you are a client of Growsin, or if you share personal or financial information with me in the context of seeking advisory or research services, your data is covered by this Policy. The protections apply across all channels, all categories of data, and all stages of the data life cycle. The only exclusions are third-party platforms that I do not control, but once the data from those platforms enters my advisory process, it comes under the same protection. The simplicity of this structure reflects the reality of a solo practice:

accountability rests entirely with me, vendors are bound to confidentiality, and clients are assured that their data will never be treated casually.

Part 3: Legal and Regulatory Framework

As an investment adviser and research analyst registered with the Securities and Exchange Board of India (SEBI), I am subject to a well-defined legal and regulatory framework that governs how I must collect, process, retain, and protect client data. This framework is not optional; it forms the backbone of my obligations as a fiduciary and is built on the principle that the relationship between adviser and client is one of trust, transparency, and accountability.

The first pillar of this framework is the SEBI (Investment Advisers) Regulations, 2013. These regulations define the responsibilities of advisers like me, and they make it very clear that I must act in the best interests of my clients at all times.

Confidentiality is not a courtesy in this context; it is a statutory duty. I am required to protect the information you provide to me and to use it only for the purposes of providing advisory services. In addition, SEBI requires that I maintain detailed records of client agreements, KYC documents, risk profiling forms, suitability assessments, investment advice, and communications with clients for a minimum of five years. This retention requirement ensures that there is always an auditable trail,

both to protect clients and to enable regulators to verify compliance.

The second pillar is the SEBI (Research Analysts) Regulations, 2014. In my role as a research analyst, I must ensure that any research I publish or provide to clients is fair, objective, and free of conflicts of interest. Just

like the investment adviser regulations, the research analyst framework also imposes obligations of confidentiality. Any personal or financial data that I handle in the course of preparing or delivering research must be safeguarded, and the records of my research reports, supporting documents, and communications must also be retained for at least five years.

The third key law is the Digital Personal Data Protection Act, 2023 (DPDP Act), which modernizes India's privacy framework and establishes specific rights for clients as data principals. Under the DPDP Act, I am recognized as a data fiduciary because I determine the purpose and means of processing your personal data. This comes with responsibilities: I must process data only for lawful purposes, with a valid basis such as consent, contractual necessity, or regulatory obligation. I must collect only as much data as is necessary for the stated purpose, store it securely, and delete it once the lawful retention period expires. I must also respect your rights to access your data, correct inaccuracies, request deletion (once retention rules permit), and withdraw consent for optional services.

The DPDP Act also requires that breaches be reported. If there is ever a material data breach that risks client harm, I am obligated to notify both you and the Data Protection Board of India within 72 hours. This level of accountability ensures that you are never left in the dark and that regulators are informed promptly.

The fourth element of the framework comes from the Information Technology Act, 2000 and the Sensitive Personal Data or Information (SPDI) Rules, 2011. These rules specifically define what counts as "sensitive personal data." For me, that primarily means bank account details, UPI IDs, passwords, and authentication information used in connection with billing or refunds. The SPDI Rules require that I obtain consent before collecting such information, use it only for the intended purpose, and ensure it is stored securely. These obligations reinforce the principle that sensitive data deserves special care, above and beyond ordinary personal data.

Together, these four pillars - SEBI's investment adviser rules, SEBI's research analyst rules, the DPDP Act, and the IT/SPDI framework - create a strong, interconnected system of responsibilities. On one hand, SEBI focuses on fiduciary duty, transparency, and recordkeeping. On the other hand, the DPDP Act and IT/SPDI rules focus on

privacy, client rights, and security safeguards. When combined, they ensure that every piece of client information I handle is governed by both sector-specific obligations and general privacy protections.

It is worth emphasizing that compliance with these laws is not simply about avoiding penalties. For me, it is about upholding trust. Clients share personal and financial details that are often highly sensitive: income, liabilities, family circumstances, investment preferences. These are not just numbers on a form; they represent real lives, goals, and responsibilities. The legal framework reinforces what should already be an ethical instinct - to protect client information as carefully as I would protect my own.

Finally, while my primary obligations are under Indian law, I am mindful that some of my clients may be non-resident Indians or may interact with me from other jurisdictions. In such cases, I continue to apply the same high standards of confidentiality and security, while ensuring that the handling of data always remains compliant with Indian laws. If any cross-border data transfers are ever required, they will only take place with your explicit consent and in accordance with Indian law, as further explained in a later section of this Policy.

In summary, the legal and regulatory framework that governs Growsin is clear and comprehensive. I must maintain confidentiality under SEBI's fiduciary rules, retain records for five years, respect client rights under the DPDP Act, handle sensitive personal data responsibly under the SPDI Rules, and notify regulators in case of breaches. By operating strictly within this framework, I ensure not only legal compliance but also the preservation of trust, which is the foundation of any meaningful advisory relationship.

Part 4: Definitions

To make this Privacy Policy clear and consistent, I use a few key terms throughout. These definitions are adapted from Indian law, especially the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Information Technology Act, 2000 including the Sensitive Personal Data or Information (SPDI) Rules, 2011. They are explained here in the specific context of my work as an individual SEBI-registered adviser and research analyst under the name Growsin.

Personal Data

Personal Data means any information that can directly or indirectly identify you as an individual. In my practice, this usually includes your name, address, date of birth, nationality, contact details, or identification numbers such as PAN or Aadhaar (where legally permitted). It may also include digital identifiers such as your phone number, email address, or IP address when you interact with me online.

For example, if you sign a client agreement and provide your name, phone number, and PAN card details, all of that is classified as Personal Data because it directly identifies you.

Sensitive Personal Data or Information (SPDI)

Some categories of data are considered sensitive under Indian law and require stronger protection. In my practice, this includes information such as bank account numbers, IFSC codes, UPI IDs, passwords, or authentication codes like OTPs.

For example, if you share your bank details so that I can issue a refund, that information is SPDI. I collect such data only when necessary, use it only for the intended purpose, and store it securely.

Financial Data

Financial Data refers to the details I need to give you meaningful advice: your income, expenses, assets, liabilities, investment portfolio, and insurance coverage. This information is not always categorized by law as "sensitive," but in practice, I treat it with the same confidentiality because it reveals a great deal about your personal and financial life.

For instance, if you want advice on retirement planning, I need to know your current savings, expected retirement costs, and future contributions. That information is your Financial Data.

Data Principal

The DPDP Act defines the individual whose data is being collected and processed as the Data Principal. In this relationship, you - the client - are the Data Principal. You hold rights over your data, and I have the duty to respect those rights.

Being a Data Principal gives you the ability to ask for access, correction, deletion after retention periods, portability, withdrawal of consent, and redressal of grievances.

Data Fiduciary

The person or entity that decides how and why personal data is processed is called a Data Fiduciary. In this case, that is me, operating as Growsin. I determine why your data is collected, how it is stored, how long it is retained, and in what limited cases it may be disclosed.

Being a Data Fiduciary means I am accountable for your data at all times. I cannot collect it casually, I cannot use it for purposes beyond what I disclose, and I cannot keep it longer than the law requires.

Part 5: Categories of Data Collected

In the course of providing investment advisory and research services, I collect certain categories of information from my clients. I do not collect information casually or unnecessarily; every piece of data I

request has a clear purpose that is either required by law, essential for fulfilling the advisory agreement, or directly connected to protecting your interests as a client. In this section, I explain in detail what categories of data I may collect, why I collect them, and how they are handled. My aim is transparency: you should never be uncertain about what information I hold about you or why it is needed.

Personal Identifiers

The most basic category of data I collect is personal identifiers. This includes your full name, date of birth, gender, nationality, and residential status. It also includes your contact details such as phone numbers, email addresses, and residential addresses. These details may seem simple, but they are essential for verifying your identity, completing regulatory requirements, and maintaining clear communication channels.

For example, when you sign up for advisory services, I need your name and date of birth to establish that you are legally eligible to contract. I need your email and phone number to deliver advice, provide updates, and share reports. Your residential status - whether you are a resident Indian or an NRI - determines which tax and regulatory frameworks apply to you. In short, personal identifiers form the foundation of the advisory relationship.

KYC Documents

Under SEBI regulations, I am required to follow Know Your Client (KYC) procedures. This means I must collect government-issued documents that verify your identity and address. Common examples include PAN card, Aadhaar card (where legally permissible), passport, voter ID, or proof of address such as a utility bill or bank statement.

These documents are not optional; they are required by law before I can provide advice or research services. They also serve to protect you by reducing the risk of fraud and ensuring that advice is delivered only to the rightful individual. Once collected, these documents are stored securely and retained for five years as

required by SEBI. After that period, they are deleted unless another law requires longer storage.

Financial Information

Because my role is to provide tailored investment advice, I need to understand your financial situation in detail. I therefore collect financial information, which may include income, expenses, assets, liabilities, investment portfolios, and insurance policies. Without this information, I cannot fulfill my fiduciary duty to provide suitable advice that matches your needs and risk appetite.

For example, if you are planning for retirement, I need to know what savings you have already accumulated, what your monthly contributions are, and what your expected retirement expenses might be. If you are looking for tax-saving strategies, I need to understand your income structure and the deductions available to you. The more accurate the financial information you provide, the more precise and effective the advice I can give.

Payment Data

When you pay for my services, I may need to collect certain payment-related details. This typically includes bank account numbers, IFSC codes, or UPI IDs. Importantly, I do not collect or store full debit or credit card numbers. Payment data is used only for the purpose of processing service fees or issuing refunds where applicable.

For instance, if you pay an annual advisory fee and later become eligible for a partial refund under SEBI's fee rules, your bank details will be used only to process that refund. Once the transaction is completed, the details are retained only as long as legally necessary and are then deleted.

Sensitive Personal Data (SPDI)

Some of the information I collect falls under the legal category of Sensitive Personal Data or Information (SPDI). This includes things like passwords, authentication codes, and bank details. The law requires me to treat this information with extra care, and I do so. I collect SPDI only when absolutely necessary - for example, to process a refund or to enable secure login to a client portal. I never disclose such data to unauthorized third parties, and I store it only for as long as required for its intended purpose.

Technical Data

When you interact with my website, digital portals, or emails, I may collect limited technical data. This includes IP addresses, device identifiers, browser types, and cookies. This information is not collected for marketing or profiling. Instead, it is used to ensure the security and proper functioning of my digital platforms.

For example, by monitoring IP addresses, I can detect unusual activity such as repeated failed login attempts from unexpected locations. If such activity is detected, I may temporarily block access to protect your account. Technical data is therefore an important tool for fraud prevention and system security.

Communication Records

As part of my practice, I maintain records of communications with clients. These may include emails, advisory notes, phone call summaries, grievance records, and reports shared with you. SEBI regulations require me to keep these records for at least five years. These records serve as evidence of the advice provided and help resolve any disputes or grievances that may arise.

For instance, if a client later questions whether advice was consistent with their stated risk profile, I can refer to the records to demonstrate that advice was indeed suitable. Maintaining communication records is therefore both a regulatory duty and a safeguard for both me and my clients.

Data of Minors

Occasionally, advisory services may be availed on behalf of a minor. In such cases, I collect only limited details of the minor such as name and date of birth, along with full details of the parent or guardian who acts as the decision-maker. All rights under this Policy are exercised by the guardian.

Exclusions

Finally, it is important to note what I do not collect. I do not collect data that is unnecessary for advisory or research purposes. I do not collect personal data from social media interactions unless you explicitly bring that information into the advisory process. I also do not collect or store biometric data, except to the extent that it may be included in a government-issued KYC document such as Aadhaar.

Part 6: Lawful Basis of Processing

The law is very clear that personal data cannot be collected or processed without a lawful reason. As someone registered with SEBI as both an investment adviser and a research analyst, I take this obligation seriously. I do not ask for or retain information unless I have a clear and valid reason, and I make sure that clients understand why their information is required. The guiding principle here is purpose limitation: I only collect data for specific purposes, and I only use it in ways that are consistent with those purposes.

Under the Digital Personal Data Protection Act, 2023 (DPDP Act) and SEBI regulations, there are four main lawful bases under which I may process client data: consent, contractual necessity, regulatory obligation, and legitimate interest.

Each of these has a distinct role, and together they cover all the situations in which I handle information.

Consent

Consent is the most familiar and direct lawful basis. It means that I will only process your information when you have freely and clearly agreed to it. Consent under the DPDP Act must be informed, specific, and unambiguous. I cannot assume consent just because you are engaging with me; I must explain what data I am collecting, why I need it, and how I will use it, and then you must agree.

For example, if I want to send you newsletters, research updates, or invitations to optional webinars, I will only do so if you have specifically opted in. Similarly, if I collect sensitive personal data like your bank account details for the purpose of issuing a refund, I will request your consent and explain exactly why the information is needed.

You also have the right to withdraw your consent at any time. If you initially agree to receive newsletters but later decide you no longer want them, you can simply withdraw your consent, and I will stop sending them. Withdrawal of consent does not affect activities that are required under law or contract, but it ensures that you have ongoing control over optional data uses.

Contractual Necessity

Some data processing is necessary for me to fulfill my obligations under the advisory or research agreement you sign with me. Without certain information, I cannot perform my services properly, and therefore this processing is justified as a matter of contractual necessity.

For example, in order to prepare a financial plan for you, I need details about your income, expenses, investments, and goals. Without this information, I cannot fulfill my obligation to provide suitable advice. Similarly, to deliver research reports to you, I need your email address or another contact method. These are not optional - they are fundamental to the service you are engaging me to provide.

Contractual necessity also applies to payments and refunds. If you pay an advisory fee, I may need to collect certain bank or UPI details to process the payment or issue a refund. This processing is part of carrying out the agreement between us and is therefore lawful.

Regulatory Obligation

As a SEBI-registered adviser and analyst, I am bound by regulations that require me to collect and retain certain information. These regulatory obligations take precedence even over individual client requests in some cases.

For instance, SEBI requires me to maintain records of client agreements, KYC documents, risk profiling forms, advice given, and related communications for a minimum of five years. Even if you ask me to delete this information earlier, I cannot

do so until the mandatory retention period has expired. This is not a matter of choice but of compliance with the law.

Regulatory obligations may also require me to disclose information to authorities. If SEBI, the Financial Intelligence Unit (FIU-IND), or the Income Tax Department requests specific records, I am legally required to provide them. Similarly, if a court issues an order for disclosure, I must comply. These obligations are not discretionary, and clients are informed of them in advance through this Policy.

Legitimate Interest

There are some situations where processing is necessary for my legitimate interest as an adviser, provided it does not override your rights. This basis is recognized under the DPDP Act and allows for certain uses that are important for security and efficiency.

For example, I may collect technical data such as IP addresses or device identifiers to monitor for suspicious activity on my website or client portal. This helps protect your account from unauthorized access. I may also use anonymized financial data to analyze overall trends in client portfolios, which in turn helps me improve

the quality of my advisory services.

Another example of legitimate interest is fraud prevention. If I notice unusual transaction activity, I may temporarily hold or review the data to ensure there is no risk to you or to the integrity of the advisory process.

In all such cases, I balance my legitimate interest against your rights as a client. If I determine that the risk to your rights outweighs the benefit of the processing, I will not proceed.

Combined Effect

In practice, these lawful bases often work together. For instance, when you sign up as a client, I process your personal identifiers under contractual necessity, your KYC documents under regulatory obligation, and your financial details under both contractual necessity and legitimate interest. If I also send you a newsletter, that part of the processing is based on your consent.

This layered approach ensures that all data processing has a solid legal foundation. There are no gaps, no assumptions, and no casual uses of client data. Each action I

take with your information can be traced back to one of these lawful bases, and you can always ask me to explain which basis applies in your case.

Part 7: Purpose of Processing

When I collect and use client data, I do so only for clear and specific purposes. I do not gather information out of curiosity, nor do I store it indefinitely without reason. Every detail you share with me is tied to a legitimate need that either enables me to provide investment advisory and research services or ensures compliance with the legal framework that governs my practice. In this section, I explain the key purposes for which I process client information.

Delivering Advisory and Research Services

The primary reason I collect personal and financial information is to provide tailored investment advice and research insights. Investment advisory is not a one-size-fits-all exercise. To recommend strategies that are suitable, I must understand your individual financial circumstances, goals, and risk profile. This requires information about your income, expenses, existing investments, liabilities, family responsibilities, and long-term objectives.

For example, if your goal is to fund your child's education abroad, I may analyze your current savings, estimate the future cost of tuition and living expenses, and

recommend an investment strategy that balances growth with risk. If your concern is wealth preservation, I may advise on a portfolio designed to minimize volatility. In both cases, I rely on your financial and personal information to provide meaningful and actionable advice. Without access to this data, the quality and suitability of my recommendations would be compromised.

Similarly, in my role as a research analyst, I provide insights into financial instruments, sectors, and market trends. While these reports may not always require personalized financial data, they are often shared in the context of a client relationship. Keeping a record of when and how such research is provided is part of ensuring transparency and accountability, as required under SEBI's regulations.

Compliance with SEBI and Other Legal Obligations

Another key purpose for processing client data is to comply with my regulatory obligations. SEBI mandates that I maintain detailed records of client agreements, KYC documents, risk profiling exercises, advice given, and communications for at least five years. These records are not only a legal requirement but also a safeguard for both clients and advisers. They ensure that there is always a reliable reference point if questions arise about the suitability of advice or the terms of an agreement.

For example, if SEBI conducts an inspection, I must be able to produce copies of the client agreements and supporting documents to demonstrate compliance. If a client disputes whether advice was consistent with their risk profile, the records provide evidence of what was shared and agreed upon. By retaining this information as required, I fulfill my legal duty and preserve a transparent advisory process.

Billing and Payment Processing

I also process client data for the purpose of billing and payment. This includes generating invoices, receiving advisory fees, and, where applicable, issuing refunds in accordance with SEBI's rules on fee structures. To complete these transactions, I may require bank account details, UPI IDs, or other payment identifiers.

For example, if you pay an annual advisory fee and later terminate the service before the end of the period, I may need to issue a prorated refund. In such a case, your payment details are used solely for processing the refund. They are not used for any other purpose and are not shared with unauthorized parties.

Communication with Clients

Effective communication is central to the adviser-client relationship. I use your contact details to share advisory notes, research reports, portfolio reviews, updates on regulatory changes, and other service-related information. Communication may take place through email, phone calls, video conferencing, or secure digital platforms.

For example, if SEBI issues a new regulation that affects your investments, I may send you an update explaining its implications. If I prepare a personalized financial plan for you, I will deliver it through your preferred communication channel.

Communication is also essential for maintaining an ongoing dialogue so that advice can be adjusted as your circumstances evolve.

Handling Grievances

Another important purpose of processing client data is to handle grievances and concerns. If you raise a complaint or express dissatisfaction with any aspect of my services, I will use your records and communications to investigate and respond.

For instance, if you believe that advice provided was inconsistent with your risk profile, I may review past communications, agreements, and financial data to address the concern. The grievance-handling process requires me to have accurate records so that I can provide clear explanations and, where appropriate, corrective action.

Fraud Prevention and Security

Finally, I process certain types of data to prevent fraud and ensure the security of my services. This includes monitoring for suspicious activity, such as repeated failed login attempts or unusual payment patterns. Technical data such as IP addresses and device identifiers may be collected for this purpose.

For example, if someone tries to access your account from an unexpected location, I may temporarily block the attempt and notify you. These security measures protect both your data and the integrity of the advisory process.

What I Do Not Use Data For

It is equally important to clarify what I do not use your data for. I do not sell client data to marketers, advertisers, or third parties. I do not use your financial information for any purpose unrelated to advisory or research services. I do not

profile you for unrelated commercial purposes. The use of your data is limited strictly to the purposes described above.

Bringing It All Together

In short, the purposes for which I process client data can be summarized as follows: delivering high-quality advisory and research services, complying with SEBI and legal obligations, managing billing and payments, communicating effectively with clients, resolving grievances, and preventing fraud. Each purpose is legitimate, necessary, and aligned with the principle of protecting client interests. By limiting processing to these defined purposes, I ensure that your information is never misused or treated casually.

Part 8: Data Retention

When clients share their personal and financial information with me, they often wonder how long I will keep that data. Retention is an important part of data protection because it balances two competing needs: on the one hand, regulators like SEBI require that records be preserved for a minimum period so that advice can be audited or verified if necessary; on the other hand, clients have a right to expect that their data will not be stored indefinitely once it is no longer required. This section explains my approach to data retention and how it works in practice.

The Five-Year Rule

Under the SEBI (Investment Advisers) Regulations, 2013 and the SEBI (Research Analysts) Regulations, 2014, I am required to retain certain categories of records for at least five years. These include client agreements, KYC documents, risk profiling forms, suitability assessments, investment advice given, research reports, and communications with clients. The purpose of this requirement is to create a reliable audit trail that protects both the client and the adviser.

For example, if a client later claims that advice given in year one was not suitable, I can refer to the documents retained to demonstrate that the advice matched the risk profile recorded at the time. Similarly, if SEBI conducts an inspection in year three, I can produce all required documents to confirm compliance. The five-year retention period ensures continuity and accountability.

Retention Beyond Five Years

In some cases, data may need to be retained for longer than five years. This usually happens when a legal dispute, regulatory inquiry, or tax matter is ongoing. For example, if a client raises a grievance in the fifth year of the advisory relationship, the related documents may need to be retained until the grievance is resolved, even if that extends beyond the five-year mark. Similarly, if SEBI or the Income Tax Department initiates an investigation, records must be preserved until the matter is closed.

I only extend retention when it is legally necessary. Once the reason for keeping the data beyond five years no longer applies, the data is securely deleted or anonymized.

Deletion and Secure Disposal

When the retention period expires, I take steps to ensure that data is securely removed. For digital records, this means permanent deletion from servers and storage systems. For physical records, it means secure shredding and disposal. The goal is to ensure that client information does not remain accessible once it no longer serves a lawful purpose.

For example, if I have retained a scanned copy of your PAN card for five years as part of KYC compliance, and there is no ongoing investigation or dispute, that document will be deleted from digital storage systems at the end of the period. This process reduces the risk of data being exposed or misused in the future.

Different Retention Periods for Different Categories

Not all categories of data are treated the same. While SEBI mandates five years for core records, some categories may be retained for shorter periods if they are not subject to regulatory requirements.

Payment details: Bank account numbers or UPI IDs used for processing payments or refunds are retained only until the transaction is complete and reconciled with financial records, unless required for tax or regulatory purposes.

Technical data: IP addresses or device identifiers collected for fraud prevention may be retained for shorter periods, typically only as long as necessary for monitoring and security analysis.

Optional communications: If you consent to receive newsletters or updates, your email address is retained for as long as you remain subscribed. If you withdraw consent, your details are removed promptly.

This flexible approach ensures that data is not held longer than necessary for its purpose.

Balancing Retention with Client Rights

The DPDP Act emphasizes that data should be retained only for as long as it is necessary for the purpose for which it was collected. My practice aligns with this principle by setting clear timelines and conditions. At the same time, I must balance these rights with my regulatory obligations. For example, even if you request deletion of your records after two years, I cannot comply until the mandatory five- year SEBI retention period has expired. Once that period ends, I honor requests for erasure promptly.

Client Awareness

Transparency is central to retention. I want clients to know exactly how long their information will be stored and under what conditions it will be deleted. This Policy itself serves as a disclosure, and clients may also contact me at any time to ask about the status of their data. If a retention extension is necessary due to legal or regulatory reasons, I will provide an explanation.

Why Retention Matters

It may seem like retention is only about rules and timelines, but in practice it plays a key role in protecting clients. By maintaining records for five years, I can demonstrate that I provided advice responsibly, that I honored my fiduciary duty, and that communications were consistent with agreements. At the same time, by

deleting data once retention obligations expire, I protect clients from the risk of unnecessary storage.

In Summary

My retention policy is simple and client-focused:

I keep data for five years, as required by SEBI.

I keep it longer only if legally necessary.

I delete it securely once it is no longer needed.

I remain transparent about how long your data is stored.

This approach ensures that retention serves its intended purpose - accountability, compliance, and protection - without turning into indefinite storage that undermines privacy.

Part 9: Data Sharing and Disclosure

Clients often ask me under what circumstances their personal or financial information might be shared with others. The answer is straightforward: I share client data only when it is legally required, operationally necessary, or when you have expressly consented to it. I do not sell or trade data, nor do I share it casually with third parties. This section explains in detail the limited situations where disclosure may occur and the safeguards around it.

Disclosure to Regulators

As a SEBI-registered investment adviser and research analyst, I am directly regulated by the Securities and Exchange Board of India (SEBI). SEBI requires me to maintain detailed records for at least five years and to provide those records on demand during inspections, audits, or investigations.

For example, if SEBI decides to review my practice, they may ask for copies of client agreements, advisory notes, or KYC documents. In such cases, I am obligated to share those records. Similarly, if the Financial Intelligence Unit (FIU-IND) requests information related to anti-money laundering requirements, I must provide it. The Income Tax Department may also require disclosure for tax compliance purposes.

These disclosures are not discretionary - they are mandatory under Indian law. When I share information with regulators, I provide only what is specifically requested and no more.

Disclosure to Courts or Law Enforcement

Another situation where disclosure may be required is when a court of law or a law enforcement agency issues a valid order. If I receive a summons, warrant, or lawful direction, I am legally bound to comply. This might involve providing certain client records or communication logs.

For example, if a court is handling a dispute involving one of my clients and orders me to produce advisory records, I must comply. Similarly, if a law enforcement agency investigates suspected fraud or financial crime, I may be required to provide information. Again, disclosure in such cases is limited to what the law specifically demands.

Disclosure to Banks and Payment Processors

When clients pay for services or receive refunds, certain information must be shared with banks or payment processors to complete the transaction. This usually includes bank account details, IFSC codes, or UPI IDs.

For example, if you pay your advisory fee through a UPI transfer, the transaction naturally involves your UPI ID being processed by the payment gateway and your bank. If a refund is issued, your bank details are used to credit the amount. Such disclosures are routine, secure, and limited to the purpose of processing payments.

Disclosure to Vendors

I rely on certain vendors to deliver services effectively. These may include hosting providers who maintain my website or client portal, cloud storage services that hold encrypted records, and payment gateways that process transactions. Vendors are permitted to handle client data only for the specific services they provide, and they are required to maintain confidentiality and implement reasonable safeguards.

For example, if I use a cloud service to store encrypted copies of client agreements, the provider hosts the data but has no right to use it for its own purposes. Similarly, if I use a payment gateway, the provider processes your payment securely but cannot access or retain your information for anything beyond the transaction.

No Marketing or Unrelated Sharing

It is equally important to clarify what I do not do. I do not share client data with marketers, advertisers, or unrelated businesses. Your personal and financial information is not used to create mailing lists for third parties. It is not analyzed for commercial gain outside of my advisory and research services. The only purposes for which your data may be disclosed are those listed above.

Limited Nature of Disclosures

Even when disclosure is required, I share the minimum amount of information necessary. If SEBI requests advisory agreements, I will not provide unrelated communications. If a court requests a specific record, I will provide only that record. This principle of minimization ensures that your information is not unnecessarily exposed.

Client Awareness

Whenever possible, I aim to keep clients informed about disclosures. If SEBI conducts a general inspection, you may not receive an individual notice because it is part of routine regulation. But if your information is specifically involved in a disclosure to a court or another authority, I will inform you unless the law prohibits me from doing so.

Why Disclosure Matters

Disclosure is not something I take lightly. However, it is sometimes unavoidable because I operate in a regulated industry. Regulators, courts, and payment systems are integral to maintaining the integrity of financial services. By limiting disclosure to

these contexts and ensuring confidentiality safeguards, I protect your privacy while fulfilling my obligations.

In Summary

The situations where I may disclose client data are limited to:

Regulators - SEBI, FIU-IND, Income Tax Department, or other statutory authorities.

Courts or Law Enforcement - when directed by lawful order.

Banks/Payment Processors - for service fee payments and refunds.

Vendors - hosting, cloud, or payment services, with confidentiality safeguards.

Outside of these contexts, your information remains strictly confidential. I do not share it for marketing, advertising, or unrelated purposes.

Part 10: Data Security

The security of client data is one of the most important responsibilities I carry as an investment adviser and research analyst. When you share your personal and financial information with me, you trust that it will be protected against loss, unauthorized access, misuse, or disclosure. I take this obligation seriously and use practical, effective safeguards to keep your information safe. In this section, I explain how I secure your data, what protections are in place, and what steps I take if a breach ever occurs.

My Approach to Security

Growsin is an individual advisory practice, which means that only I access and process client information. This structure itself reduces the risk of unauthorized access because there are no employees, associates, or teams who might mishandle data. The fewer people who have access, the lower the chance of mistakes or misuse. If I ever engage support staff in the future, they will be strictly bound by confidentiality and permitted to handle data only to the extent necessary.

Encryption and Secure Servers

Digital security begins with where data is stored. Client records such as agreements, KYC documents, and financial plans are stored on secure servers. These servers are protected by encryption, meaning that even if someone were to gain unauthorized access, the data would be unreadable without the correct decryption key. Encryption adds a strong layer of protection, especially for sensitive personal data like bank account details or authentication codes.

For example, if I hold a scanned copy of your PAN card for KYC purposes, it is stored in encrypted form on a secure server. If the server were ever compromised, the file would be useless to anyone without the correct credentials.

Password Protection

Access to systems that hold client data is restricted by strong password protection. I do not use simple or easily guessed passwords; instead, I rely on long, unique combinations that are updated regularly. Password protection is a simple but effective way to ensure that unauthorized individuals cannot gain access to my systems.

For example, if I access your financial plan through my secure portal, I use credentials that are not shared with anyone else. No third party has access to these accounts, and I take care to keep login information confidential at all times.

Limited Vendor Access

In some cases, vendors such as hosting providers, cloud storage services, or payment gateways may handle client information. These vendors are included in my security practices because they are necessary to deliver services. However, their access is limited, and they are required to maintain confidentiality and implement reasonable safeguards.

For instance, a cloud storage provider may host encrypted copies of advisory agreements, but the provider cannot view or use the data for any other purpose. A payment gateway may process your fee payment, but it cannot store or repurpose your bank details beyond the transaction. Vendors handle data only as required to provide their service, and I remain accountable for ensuring that safeguards are followed.

Physical Security

Although most client information today is handled digitally, there may be occasions when physical records are created, such as signed agreements or printed financial documents. In such cases, I store physical copies securely, away from public access, and ensure that they are disposed of responsibly once they are no longer required. For example, expired paper records are shredded rather than discarded, ensuring that sensitive details cannot be reconstructed.

Breach Response and Notification

Despite best efforts, no system is completely immune from risks. If a data breach ever occurs - whether through unauthorized access, accidental disclosure, or system compromise - I have a simple but firm response process.

First, I will act immediately to contain the breach, such as by restricting access or isolating affected systems.

Second, I will investigate the scope and impact of the breach to determine what data was involved and how it was accessed.

Third, if the breach is material and poses a risk to clients, I will notify both the

affected clients and the relevant authorities within 72 hours, as required under the DPDP Act.

For example, if someone attempted to hack into my system and accessed communication records, I would inform the clients affected, explain what happened, describe what steps were being taken to fix it, and notify the Data Protection Board of India. Transparency in such situations is essential to maintaining trust.

Ongoing Care

Security is not a one-time exercise but an ongoing responsibility. I regularly review my security practices to ensure they remain effective against new risks. This does not mean adopting complex corporate frameworks but rather applying practical, sensible measures suited to a solo practice. By keeping systems updated, using

encryption, restricting access to myself, and working only with trusted vendors, I create a secure environment for client data.

What I Do Not Do

It is also important to clarify what I do not do. I do not leave sensitive client data stored in unprotected systems. I do not share passwords with anyone. I do not allow vendors to use client data for their own benefit. And I do not ignore security updates or vulnerabilities. My approach is cautious and protective because I understand that even small lapses can have significant consequences when financial data is involved.

In Summary

My security practices are simple but effective: encryption, secure servers, strong password protection, limited vendor access, physical safeguards, and transparent breach reporting. As the sole adviser at Growsin, I am personally accountable for protecting your data. This direct responsibility, combined with straightforward security measures, ensures that your personal and financial information remains safe throughout the course of our relationship.

Part 11: Client Rights

As a client of Growsin, you do not lose control over your personal and financial information when you share it with me. Indian law, especially the Digital Personal Data Protection Act, 2023 (DPDP Act), recognizes you as the Data Principal, and it grants you specific rights over your data. I, as the Data Fiduciary, am required to respect and enable those rights. In practice, that means you can always ask what data I hold, request corrections, insist on deletion after retention periods, and raise grievances directly with me. Because Growsin is a solo practice, there are no layers of committees or compliance officers - I personally handle all such requests.

Right to Access

You can ask what data I hold about you. This includes knowing the categories of data collected, how it is being used, and whether it has been disclosed to any regulators or vendors. Transparency is the foundation of this right.

Right to Correction

You can ask me to correct or update inaccurate information. For example, if your address changes or your income records are outdated, you can request a correction. I usually make corrections within 15-30 business days.

Right to Erasure

You can ask me to delete your personal data, but this is subject to SEBI's rule that certain records must be retained for five years. After that period ends, I will securely delete or anonymize your records unless another law requires longer retention.

Right to Data Portability

You can ask for your data in a format that can be transferred to another SEBI-registered adviser. This ensures you are never locked into my services simply because I hold your records.

Right to Withdraw Consent

If you have given consent for optional uses - such as receiving newsletters or educational updates - you may withdraw it at any time. Once you withdraw, I will stop processing your data for that purpose immediately.

Right to Restrict Processing

You can ask me to pause the use of your data in specific situations, such as when there is a dispute over accuracy or if you object to how it is being used. Restriction means the data is held securely but not actively used until the issue is resolved.

Right to Grievance Redressal

You can raise grievances directly with me by emailing privacy@growsin.in. I personally review each complaint and respond within 15-30 business days. If you are not satisfied, you may escalate to SEBI through the SCORES platform or to the Data Protection Board of India for privacy-related issues.

How Requests Are Handled

When you exercise a right, I will first acknowledge your request to confirm it has been received. Then, I will review the relevant records and respond with a clear outcome - whether it is providing access, correcting inaccuracies, deleting data after the lawful period, or explaining why certain information must be retained under SEBI rules.

For example, if you request deletion after three years, I will explain that I must legally retain your records for five years but will delete them as soon as the requirement expires. This ensures clarity and avoids misunderstandings.

Simplicity of a Solo Practice

In many firms, exercising rights involves going through departments, filing forms, or dealing with compliance officers. At Growsin, the process is direct: you contact me, and I handle your request personally. This reduces delays, avoids miscommunication, and ensures that accountability rests entirely with me.

Why These Rights Matter

Your rights are not just legal formalities; they are tools that give you control. They ensure that your data is not locked away in someone else's system indefinitely. They allow you to correct inaccuracies that could affect financial advice. They guarantee eventual deletion once obligations expire. And they give you a direct voice if you believe something has gone wrong.

In Summary

As a client, your rights under this Privacy Policy include:

Access → You can ask what data I hold about you.

Correction → You can ask me to update inaccuracies.

Erasure → After 5 years, you can request deletion.

Portability → You can request your data in a transferable format.

Withdraw Consent → You can stop optional uses like newsletters.

Restrict Processing → You can ask me to pause data use in disputes.

Grievance Redressal → You can contact me at privacy@growsin.in for resolution.

I respect all these rights not only because the law requires it but because they strengthen the trust between us.

Part 12: Breach Management

No matter how careful one is, the reality of the digital world is that breaches can still occur. A breach may happen due to unauthorized access, accidental disclosure, technical compromise, or even human error. While I take strong precautions to protect your information, I also recognize the importance of having a clear and honest plan for how to respond if something ever goes wrong. In this section, I explain what I mean by a breach, how I would detect and contain one, what steps I would take to notify clients and regulators, and how I would remedy the situation while keeping you informed.

What Is a Breach?

A breach occurs whenever personal or financial data is accessed, disclosed, altered, or lost without authorization. Breaches can be deliberate, such as hacking or phishing attacks, or accidental, such as sending a file to the wrong email address. A breach does not have to involve large volumes of data - even a single unauthorized disclosure is treated as a breach.

For example, if someone were to gain unauthorized access to a client agreement stored on my server, that would qualify as a breach. Likewise, if an advisory note were mistakenly sent to the wrong client, I would treat it as a breach. Recognizing breaches quickly and acting decisively is essential for protecting clients.

Detection

As a solo adviser, I monitor my own systems and communications closely. Because I am the only one who accesses and processes client information, I am usually the first to spot any irregularity. I also rely on alerts from vendors such as hosting providers or payment gateways, who are required to notify me if they detect unusual activity.

For example, if my hosting provider notices multiple failed login attempts from an unfamiliar location, I would treat that as a potential breach and investigate immediately. Clients can also help by notifying me if they notice anything unusual, such as receiving a suspicious email that appears to come from me.

Containment

The first step after detecting a breach is containment. This means preventing further unauthorized access or disclosure. Depending on the situation, containment may involve isolating affected systems, changing passwords, revoking access, or disabling a compromised account.

For example, if I discovered that my email account was compromised, I would immediately reset the credentials, enable stronger protections, and review sent messages to identify any affected clients. The goal of containment is to stop the breach from spreading and to limit its impact.

Notification Within 72 Hours

Under the Digital Personal Data Protection Act, 2023 (DPDP Act), material breaches that pose a risk to client rights must be reported to the Data Protection Board of India and to affected clients within 72 hours of detection. I fully comply with this requirement because transparency is essential in such situations.

For example, if client financial records were accessed due to a technical compromise, I would notify the affected clients as soon as possible, explain what happened, outline the potential risks, and describe what steps were being taken to address the issue. At the same time, I would notify the Data Protection Board of India, ensuring that regulators are aware and can provide oversight.

Remediation

After containment and notification, the next step is remediation. This means fixing the cause of the breach and taking corrective measures to prevent recurrence.

Remediation may include applying security patches, changing vendors, improving access controls, or adding new layers of protection.

For instance, if a breach occurred because of a weakness in my hosting provider's system, I might migrate to a more secure provider and strengthen encryption standards. If the breach was due to a misdirected email, I would adopt stricter review practices before sending sensitive files.

Compensation and Responsibility

As the sole adviser operating under Growsin, I take full responsibility for protecting client data. If a breach occurs due to my negligence and causes harm to a client, the DPDP Act gives clients the right to seek compensation. I recognize this accountability,

and it guides my cautious approach to data handling. At the same time, it is important to note that not all breaches are preventable - for example, if they arise from circumstances beyond anyone's reasonable control, such as natural disasters or acts of terrorism.

Client Reassurance

Perhaps the most important part of breach management is client reassurance. A breach can cause anxiety, even if no actual harm results. By acting quickly, communicating openly, and demonstrating that concrete steps are being taken, I aim to reassure clients that their interests remain protected. Transparency builds trust, and trust is the foundation of my advisory practice.

In Summary

My breach management process is simple but firm:

Detect irregularities quickly through personal vigilance and vendor alerts.

Contain the breach to prevent further damage.

Notify affected clients and regulators within 72 hours, as required by law.

Remediate the issue by fixing vulnerabilities and strengthening protections.

Reassure clients through transparency and accountability.

By preparing for the possibility of a breach, I make sure that even in the worst-case scenario, your interests are protected and your trust is respected.

Part 13: Cross-Border Data Transfers

In today's financial and digital environment, it is common to hear about data flowing across borders, stored in servers located around the world, or processed by multinational vendors. At Growsin, my approach is deliberately simpler and stricter: by default, all client data is stored in India. I make every effort to keep personal and financial information within Indian jurisdiction, governed by the same laws and regulations that apply to my advisory practice.

Default Approach: All Data Stored in India

The first and most important point is that your data - whether it is your KYC documents, client agreements, financial records, or advisory notes - is stored securely on servers located in India. By keeping data local, I ensure that it remains protected by Indian privacy laws, SEBI regulations, and the Digital Personal Data Protection Act (DPDP Act). This also gives clients reassurance that their data is not being moved around internationally without their knowledge or consent.

For example, when you share your PAN card for KYC verification or provide details about your financial goals, those records are encrypted and stored in Indian servers. They are not transferred abroad automatically or by default.

Limited Exceptions

There are some limited circumstances where a cross-border transfer may be necessary, though these are rare and always handled cautiously.

NRI Clients: If you are a non-resident Indian and request that I share certain documents with your overseas tax adviser or financial consultant, I may transfer your information outside India - but only with your explicit consent.

Vendor Infrastructure: Some service providers, such as global payment gateways or hosting services, may have technical systems that store or mirror data outside India. If this becomes necessary for the delivery of

services, I will inform you in advance and seek your consent.

Client Requests: If you specifically ask me to share information abroad - for example, sending financial records to a foreign bank you work with - I will do so only after explaining the purpose and receiving your clear approval.

Outside of these limited cases, your information will not leave India.

Explicit Consent Is Required

A key safeguard is that no data transfer abroad happens without your explicit consent. Consent means that I explain what information will be transferred, to whom, and why - and you agree to it. This ensures that you always remain in control of your personal and financial data.

For example, if you request me to share your investment plan with an overseas adviser, I will not simply forward it. I will ask you first to confirm in writing or over email that you want this transfer to occur. Only then will I proceed.

Compliance with Indian Law

Even when transfers do occur, they are governed by Indian law. The DPDP Act requires that data be processed lawfully, securely, and only for the purposes consented to by the client. I comply with these requirements fully. If the Indian government restricts transfers to certain jurisdictions, I will follow those restrictions.

This means that even if you request a transfer abroad, I will only carry it out if it does not conflict with Indian legal requirements. My priority is always to ensure compliance first, followed by client consent.

No Routine or Automatic Transfers

It is equally important to clarify what I do not do. I do not routinely send data abroad. I do not use foreign analytics companies or marketing services that extract client information. I do not allow vendors to move your financial details into international databases without reason. Transfers are not automatic - they happen only when necessary and always with your approval.

Transparency With Clients

If a transfer ever does occur, I make sure clients are informed clearly. You will know what is being transferred, why it is being transferred, and how it will be used. There are no hidden flows of data. By being upfront about such situations, I maintain transparency and ensure that your trust is never compromised.

Bringing It Together

In practice, this means that nearly all my work with clients happens with data stored entirely within India. Your agreements, your KYC records, your financial details, and our communications are retained locally, secured by Indian law. Only if you are an NRI client who requests an international transfer, or if a critical vendor system requires it, would data ever leave the country - and even then, only after you provide explicit consent.

In Summary

My approach to cross-border data transfers is simple and client-focused:

All data is stored in India by default.

Transfers abroad are rare and happen only when necessary.

No transfer occurs without your explicit consent.

Transfers always comply with Indian law.

No routine or unnecessary transfers are made.

This ensures that your personal and financial information remains under the protection of Indian law while giving you control in the rare event that data must be transferred abroad.

Part 14: Enforcement and Accountability

Privacy policies and data protection frameworks only have meaning if someone takes responsibility for ensuring they are followed. In large organizations, this responsibility may be spread across compliance officers, IT teams, and internal committees. At Growsin, things are much simpler: I am personally responsible for every aspect of data handling, and I am directly accountable to my clients and to regulators. This section explains how accountability works in practice, what it means for clients, and how I enforce the commitments made in this Privacy Policy.

Sole Responsibility

As an individual adviser, I alone collect, process, store, and disclose client data. This concentration of responsibility eliminates ambiguity. There is no question of whether a junior associate misused data or whether a compliance officer failed to monitor safeguards - because there are no such intermediaries. Every piece of information you share is handled by me directly, and I am accountable for it.

This structure may appear simple, but it is also powerful. By eliminating multiple access points and concentrating responsibility in a single person, I reduce the risk of data leakage or mishandling. It also strengthens accountability because I cannot shift blame to a team or department. The responsibility begins and ends with me.

Transparency with Clients

Accountability is not just about internal responsibility; it also requires transparency toward clients. That is why I make this Privacy Policy detailed and comprehensive. Clients should never have to guess what happens to their information. If you want to know what data I hold, why it is being retained, how it is being used, or whether it has ever been disclosed to a regulator, you can ask me directly.

For example, if you write to me at privacy@growsin.in requesting details of your retained records, I will provide a clear explanation. If your information was shared with SEBI or another regulator as part of a lawful inspection, I will tell you what was disclosed and why. This openness builds trust and ensures that accountability is not hidden behind vague promises.

Enforcement by Law

My accountability is not only personal but also legal. As a SEBI-registered investment adviser and research analyst, I am bound by the SEBI Regulations, the DPDP Act, and the IT Act with SPDI Rules. These laws create clear obligations for me and empower regulators to enforce them. If I fail to comply with these rules, SEBI or the

Data Protection Board of India can take action, which may include penalties or even cancellation of registration.

For example, if I were to ignore a client's request to correct inaccurate data, I could be held in violation of the DPDP Act. If I failed to retain records for the required five years, SEBI could penalize me for non-compliance. This external enforcement reinforces my internal commitment to do things properly.

Direct Client Recourse

Clients also have direct recourse if they believe I have not lived up to my obligations. You may raise grievances with me directly, and if you remain dissatisfied, you can escalate the matter to SEBI through the SCORES platform or to the Data Protection Board of India for privacy-related concerns. This means that

accountability does not depend solely on my assurances; it is backed by external mechanisms that clients can rely on.

For instance, if you request erasure of your records after the five-year retention period has expired and I fail to comply, you can approach the Data Protection Board of India to enforce your right. Knowing that such mechanisms exist keeps me vigilant and responsive.

Self-Enforcement Through Simplicity

One of the strengths of operating as a solo adviser is that enforcement becomes simpler. Because I am the only one handling data, enforcement is not about monitoring multiple employees or setting up internal audits. Instead, it is about maintaining discipline in my own processes and following the commitments I have made in this Policy.

For example, I know that SEBI requires retention of client agreements for five years. I therefore maintain a personal record system to ensure those documents are kept securely for the required period and deleted afterward. Similarly, I know that the DPDP Act requires breach notification within 72 hours. I therefore keep my communication channels ready so that I can notify clients immediately if something happens.

Accountability in Practice

Accountability in practice means being proactive rather than reactive. I do not wait for regulators or clients to point out lapses; I take care to avoid them in the first

place. That means securing data before a breach occurs, clarifying retention rules before deletion requests come in, and being transparent about disclosures before clients have to ask.

For example, if I anticipate that a vendor's systems may involve cross-border data storage, I inform clients in advance and seek consent, rather than waiting until after the transfer has already taken place. By treating accountability as a continuous responsibility, I reduce the chances of conflict and build stronger trust.

In Summary

Enforcement and accountability at Growsin rest on three pillars:

Personal responsibility - I alone handle client data and am accountable for it.

Legal enforcement - Regulators like SEBI and the Data Protection Board ensure compliance.

Client recourse - Clients can raise grievances directly with me or escalate externally.

This framework ensures that accountability is not just a word in a policy but a lived reality. By taking sole responsibility, remaining transparent, and aligning with legal enforcement, I provide clients with the assurance that their data is always handled carefully, lawfully, and respectfully.

Part 15: Grievance Redressal

Even with the strongest safeguards and best intentions, clients may sometimes have concerns, questions, or complaints about how their data is being handled. The law recognizes this possibility, and so do I. That is why grievance redressal forms an important part of my Privacy Policy. Clients must have a simple, direct, and effective way to raise issues, and they must be confident that their concerns will be taken seriously. As Growsin is a solo advisory practice, grievance handling is straightforward: you communicate directly with me, and I am responsible for providing a fair and timely resolution.

How to Contact Me

If you have a grievance relating to the collection, use, storage, or disclosure of your personal or financial data, you can contact me directly at privacy@growsin.in . This is the official point of contact for all privacy-related

matters. You do not need to fill out multiple forms, call a helpline, or navigate through different departments. Your grievance reaches me directly, and I take personal responsibility for addressing it.

You may also write to me by physical mail if preferred, but email is generally the fastest and most reliable way to ensure your grievance is logged promptly. Whether your concern is big or small, you can use this channel to raise it.

Acknowledgement of Grievance

Once I receive your grievance, I will send you an acknowledgment within a reasonable time. This acknowledgment is important because it assures you that your complaint has been received and is under review. I do not let grievances sit unanswered or unnoticed; I make it a priority to confirm receipt so that you know your concern is being taken seriously.

Timeline for Resolution

I aim to resolve grievances within 15 to 30 business days. The exact timeline depends on the nature of the issue. Some concerns, such as correcting an error in your contact details, can be resolved quickly. Others, such as reviewing whether data has been disclosed lawfully, may require more time. Regardless of complexity, I keep you informed of the progress and ensure that you are never left without updates.

For example, if you request correction of your income records, I can usually confirm and update them within 15 business days. If you raise a concern about whether your records were disclosed to a regulator, I may need to review correspondence and retention logs, which could take closer to 30 business days.

Steps in the Process

Grievance handling typically follows these steps:

Receipt: Your grievance is received via email or letter.

Acknowledgment: I confirm receipt and let you know the matter is being reviewed.

Review: I investigate the grievance by checking the relevant records, communications, or disclosures.

Response: I provide you with a clear written response, explaining the findings and actions taken.

Closure: Once you are satisfied, the grievance is closed. If you remain dissatisfied, you may escalate externally.

Escalation Options

If you are not satisfied with the resolution provided by me, you have the right to escalate the matter externally. For advisory-related grievances, you may approach SEBI through its SCORES platform, which is designed to handle complaints against SEBI-registered intermediaries. For privacy-specific concerns, you may escalate the matter to the Data Protection Board of India under the DPDP Act.

These escalation options exist to give clients an additional layer of protection and oversight. They ensure that even if you disagree with my resolution, you have independent authorities who can review the matter.

No Committees or Layers

Because Growsin is a solo advisory practice, grievance redressal does not involve compliance officers, internal committees, or multiple departments. You are not passed from one person to another. This simplicity is an advantage: it means that your grievance is reviewed and resolved by the same person who is responsible for data handling in the first place. There is no dilution of responsibility, and there are no bureaucratic delays.

Confidentiality of Grievances

All grievances are treated confidentially. The fact that you raised a concern will not be disclosed to third parties unless required by law. For example, if your grievance involves a suspected data breach, I may need to inform the Data Protection Board of India, but I will not share your complaint with unrelated parties. This confidentiality ensures that clients feel safe raising issues without fear of retaliation or exposure.

Why Grievance Redressal Matters

Grievance redressal is not just a compliance requirement; it is also a reflection of respect. By providing clients with a clear process and responding honestly, I demonstrate that I value their trust. Financial advisory is built on transparency, and grievance handling is part of that transparency. Clients must feel confident that their voices are heard and their concerns matter.

In Summary

My grievance redressal framework is simple but effective:

You can contact me directly at privacy@growsin.in .

I acknowledge grievances promptly.

I aim to resolve them within 15-30 business days.

I provide clear, written responses.

If you are dissatisfied, you can escalate to SEBI or the Data Protection Board.

All grievances are handled confidentially.

This straightforward process reflects the nature of Growsin as a solo advisory practice - direct, accountable, and transparent. It ensures that grievances are not only resolved but also treated as opportunities to strengthen trust and improve my services.

Part 16: Policy Updates and Client Communication

Laws, regulations, and business practices do not remain static. Over time, SEBI may amend its regulations, Parliament may update data protection laws, or new technologies may create different risks and safeguards. To remain compliant and transparent, I must occasionally update this Privacy Policy. This section explains how I approach updates, how clients will be informed, and how I ensure that communication about changes is always clear and direct.

Why Updates Are Necessary

The main reason I update this Policy is to stay aligned with the law. For example, when the Digital Personal Data Protection Act, 2023 (DPDP Act) came into effect, I revised the Policy to reflect the new rights granted to clients and the new obligations placed on advisers. Similarly, if SEBI introduces changes in the recordkeeping requirements for investment advisers or research analysts, I must reflect those changes here.

Updates may also be necessary to address new risks or practices. For example, if I begin using a new digital platform to communicate with clients or introduce a new vendor for cloud storage, I will update this Policy to explain how that platform or vendor fits into my data protection framework.

In short, updates are not made casually but only when necessary to reflect legal changes, new risks, or operational adjustments that affect how I handle client information.

How Clients Are Notified

Whenever I make a material change to this Privacy Policy, I will notify clients clearly and directly. I may do this through an email sent to your registered address, a notice posted on my website, or both. I do not believe in hidden updates or small print changes. Transparency means making sure clients know when the rules

change and giving them an opportunity to review the changes.

For example, if I update the Policy to reflect a new requirement under SEBI regulations, I will email all current clients with a summary of the change and provide a link to the updated Policy. If I add a new vendor for data processing, I will disclose that vendor's role and explain how your data will be protected.

Effective Date of Changes

Each updated version of the Privacy Policy will carry an effective date so that you can easily see when the latest changes took effect. I retain previous versions for reference so that if a question arises about how your data was handled at a certain point in time, we can refer back to the applicable version. This practice ensures continuity and accountability.

Client Consent for Material Changes

If an update involves a material change in how I handle your data - for example, if I introduce a new category of data collection or propose a new type of disclosure - I will seek your explicit consent before applying that change to your information.

For example, if I decide to start offering an optional research subscription that requires collecting new technical data, I will first explain what is being collected and why, and then ask for your consent. If you do not consent, your data will not be processed under the new terms. This ensures that you always remain in control.

Minor Updates Without Consent

Not all updates require consent. Minor clarifications, formatting improvements, or changes made solely to reflect legal obligations may be applied without asking for additional consent, though you will still be notified. For example, if SEBI changes the required retention period from five years to six years, I am legally obligated to comply and will update this Policy accordingly. In such cases, client consent is not needed, but transparency remains important, and I will inform you of the change.

Client Communication Practices

Beyond policy updates, I believe in maintaining open lines of communication with clients about data protection. If you ever have questions about how your information is being handled, you can contact me at privacy@growsin.in . If an update to the Policy is unclear, I will explain it directly rather than leaving clients uncertain.

For example, if you receive an update notice and want to know whether it affects your stored KYC documents, you can email me, and I will clarify. This proactive communication ensures that updates are not just technical documents but practical guidance you can understand.

Commitment to Transparency

Ultimately, updates to this Privacy Policy are not just about compliance. They are about trust. Clients should never feel that the rules are shifting without their

knowledge or that new practices are being introduced without consent. By committing to clear communication, timely notification, and client involvement where necessary, I aim to make policy updates a seamless part of our ongoing relationship.

In Summary

My approach to updates and client communication is guided by simplicity and transparency:

Updates are necessary when laws change, risks evolve, or new practices are introduced.

Clients are notified directly through email or website notices.

Each version carries an effective date, and past versions are retained.

Material changes require explicit consent before applying to your data.

Minor legal or formatting changes are applied transparently without new consent.

Direct communication is always available at privacy@growsin.in for clarifications.

By following this approach, I ensure that clients are never caught by surprise and that trust remains intact even as laws and practices evolve.