



Personal Information Protection Policy

Publish Date: September 22, 2025
Version:1.0

Company Confidential. Intended for internal use only. When printed or downloaded, this is an uncontrolled document that should be used for reference only. The most current version is available online.

This Policy helps the Company comply with legal or regulatory obligations and may not be substantively revised or retired without approval from the Legal and Compliance Departments.

Contents

Introduction – Statement of General Policy 3

Policy Objectives..... 3

Requirements..... 3

Definition of Terms 3

Section 1: Apex’s Legal Obligations..... 4

Section 2: Personal Information..... 5

Section 3: Inventory and Records of Processing Activities 9

Section 4: Privacy Notices..... 9

Section 5: Privacy Rights Requests 10

Section 6: Third Party Access or Receipt..... 12

Section 7: Data Protection Impact Assessments..... 13

Section 8: Privacy Principles 13

Section 9: Protection of Personal Information 15

Section 10: International Transfers 16

Section 11: Privacy Awareness Training..... 18

Section 12: Privacy Incidents..... 18

Section 13: Privacy Complaints 18

Section 14: Artificial Intelligence 19

Section 15: Contact Us..... 19

Policy Exceptions 19

Related Information..... 19

Policy Review and Approval 20

Appendix A – Personal Information..... 21

Introduction – Statement of General Policy

All employees, including full-time, part-time, and other individuals such as contractors, consultants, and other agents (“**Associates**”) of Apex Fintech Solutions Inc. and its subsidiary affiliates (collectively, “**Apex**” or the “**Firm**”), shall employ reasonable and appropriate safeguards to protect the integrity, confidentiality, and availability of all Personal Information processed by Apex.

Policy Objectives

Apex receives, creates, collects, maintains, uses, and discloses Personal Information belonging to its customers, clients, employees, service providers and other individuals. Apex is committed to protecting Personal Information against inappropriate access, exfiltration and use in compliance with applicable laws and regulations and in order to maximize trust and integrity.

Requirements

All Associates must comply with this Personal Information Protection Policy (the “**Policy**”) and any additional policies which Apex introduces. Failure to comply with this Policy may result in disciplinary action.

Definition of Terms

“**Client**” means a corporate entity or organization which Apex provides services to on a business-to-business basis. For Apex, this is typically a correspondent, advisor, introducing broker or other financial institution and includes any sub-advisors or sub-clients.

“**Customer**” means an individual who obtains or has obtained a financial product or service from Apex that is used primarily for personal, family, or household purposes, or that individual's legal representative. For Apex, this is typically non-corporate account holder(s) of a brokerage account and may otherwise be referred to as an “End Investor”.

“**Customer Information**” means Personal Information relating to Apex (or Apex's clients') individual or consumer customers. See [Section 2: Personal Information](#) for more information.

“**Incidental Processing**” means Processing of Personal Information as a secondary consequence of routine, necessary and basic business functions that are integral to standard business operations. Examples include:

- Personal Information of the sender and recipients (e.g. name and email) Processed as part of sending and receiving regular business emails
- An Associate providing their own contact information as part of inquiries about a third-party service or a conference

“Personal Information” (otherwise known as **“PI,” “PII,” “NPI,”** or **“Personal Data”**) means any information that relates to an identified or identifiable individual or (residential) household subject to Processing by Apex or any of its service providers. See [Section 2: Personal Information](#) for more information.

“Process” or **“Processing”** means any operation or set of operations performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Section 1: Apex’s Legal Obligations

A variety of laws, regulations and legal obligations apply to Apex and the data that we obtain, alter, store, share or otherwise Process that relates to individuals, which is known as *“Personal Information”* (see [Section 2: Personal Information](#) below).

Apex’s legal obligations as they relate to privacy and data protection vary depending on:

- a) the geographical location of the individual that the Personal Information relates to;
- b) the sector or industry context (e.g. financial services product, marketing or healthcare);
- c) characteristics or context of the individual (e.g. a minor, vulnerable individual, B2B contact or retail customer); and
- d) specific contractual commitments Apex has made to clients or other third parties regarding Personal Information.

Key privacy laws applicable to Apex are:

Name	Description
Regulation S-P (“Reg S-P”)	Established by the SEC and applicable to broker-dealers and other financial institutions. Reg S-P provides for the security and privacy of consumer financial information in the US.
US State Data Breach Notification Laws	Each US state has its own data breach notification law which requires notification to impacted consumers, regulators and other bodies if certain Personal Information is compromised.
California Consumer Privacy Act (“CCPA”)	A comprehensive privacy law that applies to residents of California across consumer, employment and B2B contexts.
The General Data Protection Regulation (“GDPR”)	A comprehensive privacy law that applies to all individuals within the European Economic Area and across all industries.
Lei Geral de Proteção de Dados (“LGPD”)	Brazil’s GDPR equivalent law that applies to all individuals in Brazil.

The Data Protection Act 2018 (and GDPR as implemented in the UK)	The UK's GDPR equivalent law that applies to all individuals in the United Kingdom.
Philippines' Data Privacy Act	A comprehensive privacy law that applies to Apex employees and contractor in the Philippines.

This is a non-exhaustive list. Apex is subject to other privacy laws and other legal obligations relating to Personal Information with varying requirements. As a result, the Privacy Office has rationalized Apex's requirements into one simplified approach detailed in this Policy which all Associates are required to follow.

Section 2: Personal Information

1. What is Personal Information

With rapid technological expansions driven by the internet, connected devices, big data and artificial intelligence, there has been a significant expansion in volume, types and depth of information that relate to individuals. This information is referred to as: "Personal Information".

"*Personal information*", "*personally identifiable information*" (or "*PII*"), "*personal data*," "*nonpublic personal information*" and other similar terms are all different terms used to refer to information that relates to an individual. These terms and their meanings vary across different laws and industries.

In order for Apex to meet its various legal obligations as it relates to privacy, Apex has adopted the following definition for Personal Information:

Personal Information (or "**PII**") *any information that relates to an identified or identifiable individual or (residential) household*

Any Information

Any information, no matter the form it takes or if it relates to the individual's private and family life or information regarding the working, economic or social behavior of the individual or even if the information is publicly available.

Relating to

If the information is about a particular individual. Information relating to a group of individuals (aggregated) that cannot reasonably be attributed to any one person is not Personal Information.

Identified or Identifiable

An individual is '*identified*' or '*identifiable*' if they can be distinguished from a group of other individuals. Name is a common method of direct identification, but an individual can be distinguished from others by an identifier, such as an account number or unique ID.

When considering if an individual is identifiable, Associates must also factor in the context and all of the resources available to a user or recipient to interpret, supplement or analyze the data. For example, could you use the internet or an application in combination with the data you already have to identify someone?

An individual or household can also be identified indirectly by combining data elements within a smaller dataset (e.g. ZIP code + house color + car type); and/or by context or combining data with readily available information to the recipient.

Individual or household

Information is Personal Information only if it relates to an **individual** or a residential **household**. Information about a corporation, company, institution, club, trade union or other non-individual entities or groups of individuals is not Personal Information. However, information relating to an employee or other individual of these bodies or groups is Personal Information.

Connected Information

Where Personal Information exists in a dataset, all information connected to each identifiable individual is also Personal Information. For example, where a spreadsheet separates individuals in rows by name, all information in that row that connects to the individual is also Personal Information. Context is important for establishing this.

2. Customer Information

Customer Information is Personal Information that relates to individuals who obtain financial products or services from Apex or its B2B clients. This category of Personal Information is particularly important for Apex as it represents a significant portion of the data (let alone Personal Information) maintained and processed by Apex.

Customer Information relating to US accountholders is protected by security and privacy rules under Regulation S-P and is enforced by the SEC, FINRA and other regulatory bodies. Customer Information is protected by similar rules for accountholders residing outside of the US. Customer Information is considered more sensitive than other categories of Personal Information due to its potential for its misuse to cause financial harm to consumers.

For specific information on Apex's policies and procedures in respect of Customer Information under Regulation S-P (and GLBA) please refer to the relevant Supervisory Written Procedures.

Examples of this type of information can be found in the table below in C. Examples of Personal Information at Apex.

3. Examples of Personal Information at Apex

This table provides some examples of common Personal Information types at Apex. Please note that this table is not exhaustive.

An identifier is a datapoint that alone sufficiently identifies an individual and therefore makes all information and data connected to the identifier also Personal Information.

Individual Type	Example Identifiers	Example Connected Information
Customer or End Investor (Customer Information)	a. Name b. Social Security Number c. Address d. Email Address e. Account Number f. Phone number g. Government issued ID or number h. ACH information	i. Account type ii. Suitability criteria iii. Cash balance iv. Securities purchased, held or sold v. Marital status vi. Politically exposed person status vii. Financial institution viii. Date of birth
Employees at clients, prospects or service providers	a. Name b. Business Email Address c. Instant Messaging ID d. Phone Number e. Username	i. Employer ii. Job title iii. Preferences
Applicants and employees	a. Name b. Employee ID c. Phone Number d. Email Address e. Address f. Bank Account Numbers g. HR records h. Background checks i. Fingerprints	i. Educational history ii. Past employers iii. Job title iv. Salary and pay v. Marital status

4. Personal Information Sensitivity

Personal Information must be always protected and handled with care by Associates. The level of protection and care that Associates must exercise depends on the sensitivity of the Personal Information in question.

How *sensitive* Personal Information is depends on the level of potential harm that the misuse of the Personal Information could cause to the individual it relates to or to Apex as a result of legal, regulatory, reputational or other repercussions.

Customer Information is particularly sensitive as by its nature it will typically convey information about the financial position and assets of a consumer and the misuse or inadequate protection of it can result in fraud or financial harm to consumers.

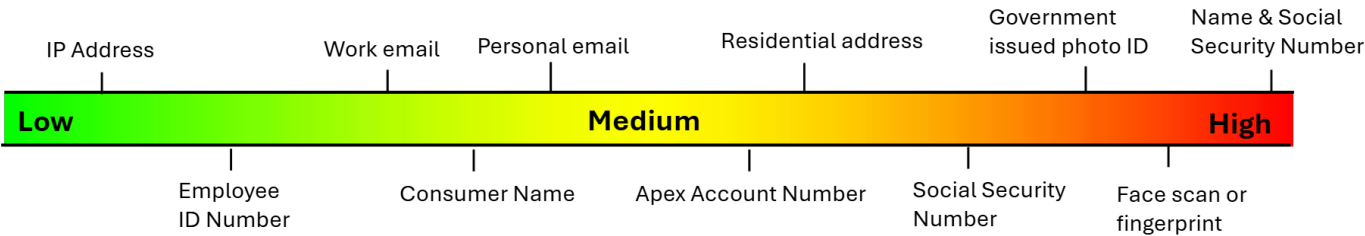
The most sensitive form of Personal Information is Sensitive Personal Information and the misuse or lack of proper protection of this information will cause significant harm to Apex and the individuals it relates to.

Sensitive Personal Information (or “SPII”)	<i>a subcategory of Personal Information that has a heightened level of sensitivity due to the harm that its misuse could cause an individual or Apex</i>
--	---

The common types of Sensitive Personal Information at Apex include:

- a) Government issued ID numbers (such as a social security, driver’s license, state identification card, alien, tax or passport number);
- b) Copy of a government issued photo ID (such as a copy of a passport, driving license or other photo ID)
- c) Any combination of information that can enable access to a consumer’s account (regardless of multifactor authentication). For example:
 - i. username/email address/account number; and
 - ii. any required security code or password to access the account.
- d) Details of citizenship or immigration status (such as nationality)
- e) Political opinions (such as politically exposed person status)

Sample Personal Information Sensitivity Scale:



For a full list of Sensitive Personal Information, please refer to Appendix A.

Section 3: Inventory and Records of Processing Activities

Apex’s Privacy Office maintains an inventory of what Personal Information Apex (including its service providers) collects, stores, shares, alters, discloses, destroys and otherwise Processes.

This inventory is not an exhaustive or conclusive repository of information, its aim is to serve as a holistic representation of the processing activities across Apex. Apex leverages this inventory to create its Records of Processing Activities (“**ROPA**”) that are required under privacy laws and used to ensure our external privacy disclosures are accurate and up to date.

Any Associates that are involved in processes to update or expand the inventory and ROPA must provide accurate and timely responses to questions, surveys and actively participate in any arranged workshops. Associates representing their departments and teams in this inventory process are responsible for the accuracy of reporting their department’s processing activities to the Privacy Office. Failure to do so may result in regulatory penalties, litigation and in Apex not having the legal rights to use Personal Information to pursue its business objectives.

Section 4: Privacy Notices

Apex is required to provide individuals with information regarding what Personal Information Apex collects, creates and receives about them along with how Apex uses, stores, shares, protects and otherwise Processes it. Apex has developed a variety of privacy notices and disclosures depending on the applicable privacy laws and the relationship Apex has with the individual.

Each privacy notice is a binding commitment by Apex to the respective individual regarding how Apex will process the individual’s data. If Apex processes Personal Information in violation of these

commitments and the reasonable expectations of an individual, Apex may be subject to regulatory or legal action. Apex's Privacy Notices include:

Type of Privacy Notice	For Whom	Primary Location
Public Privacy Notices	Customers, consumers, website visitors, employees of third parties or job applicants	Found on the relevant Apex company's website under "privacy"
Internal Privacy Notices	Associates located in the UK, Philippines or California	Provided at Associate onboarding and available on the Apex intranet

The Privacy Office is ultimately responsible for the creation, review and maintenance of all Apex privacy notices. The Privacy Office relies on timely responses from Associates, information from the ROPA and all Associates' compliance with this Policy to ensure its privacy notices are accurate, up to date and meet the requirements of privacy laws.

If the Privacy Office requests that your department update certain privacy notices on websites, the intranet, in technology, etc., please ensure you update these within a reasonable timeframe and by the deadline requested by the Privacy Office.

Section 5: Privacy Rights Requests

Various privacy laws provide individuals with certain rights regarding their Personal Information. As either a data controller or data processor under privacy laws, Apex has privacy law obligations to either directly respond to a privacy rights request (e.g. Customers located outside of the US) or to assist a client or partner in their response to a privacy rights request that they have received (e.g. Apex Silver).

Individuals' privacy rights vary depending on the applicable privacy law and certain exemptions may apply to the fulfilment of them. For example, due to US securities laws Apex Clearing Corporation may not be able to delete customer information for an open account until the account is closed and relevant retention requirements have been satisfied.

Each privacy rights request requires review to determine applicability and possible exemptions. Additionally, privacy laws set specific timeframes by which Apex must respond to a request.

Unless the Privacy Office has given prior authorization to a department to handle these rights requests, **no Associate should attempt to manage and respond to privacy rights requests**. Any privacy rights requests must be immediately escalated to Privacy Office at privacy@apexfintechsolutions.com.

The information below details the most common privacy rights and examples of what these may look like:

- 1) **Right to Access/Know:** This right provides individuals with the right to confirm if a business processes *their* Personal Information and, if so, the right to receive a copy of this Personal Information. This may look like:
 - a) “Do you have my data?”
 - b) “What type of information do you have about me?”
 - c) “I’d like a copy of all information you have on me.”
 - d) “I’d like to exercise my right to know and access my data.”
- 2) **Right to Deletion/Be Forgotten:** This right provides individuals with the right to request that their Personal Information be deleted. This may look like:
 - a) “I want to be forgotten.”
 - b) “Please delete my data.”
 - c) “Remove all of my information from your systems and databases”
 - d) “Delete my information.”
- 3) **Right to Correction/Rectification:** This right provides individuals with the right to request their Personal Information be updated where inaccurate. This may look like:
 - a) “Please update my last name to Doe”
 - b) “My address has changed to 1234 Sunny Street.”
- 4) **Right to Data Portability:** This right provides individuals with the right to have their Personal Information ported or sent to another controller or business. This may look like:
 - a) “Please send my account information to Bank ABC.”
 - b) “Please share my information with Company XYZ.”
- 5) **Right to Object to Automated Decision:** This right provides individuals with the right to opt out of automated decisions made without any human involvement. For example, an automated decision may occur if human resources leverage a resume scanning tool to automatically identify potential candidates for hire without a manual review of rejected resumes. This may look like:
 - a) “Please do not use technology to automatically make a decision about my personal information.”
 - b) “I’d like to opt out of automated decision-making.”

Section 6: Third Party Access or Receipt

Prior to providing any third party with or with access to any Personal Information (except for Incidental Processing), Apex must ensure that the access and proposed use is lawful and that appropriate contractual terms are in place with such third party, whether the third party is a client, service provider, partner or a PEAK6 affiliate. Other than Incidental Processing, Associates and Apex departments are prohibited from sharing any Personal Information with a new third party or sharing additional Personal Information through an existing third-party relationship without approval from the Privacy Office and Legal.

1. Service Providers

Service providers who process Personal Information on Apex's behalf are considered "processors" or "service providers" under applicable privacy laws that Apex is responsible for. Privacy laws mandate that Apex puts in place contractual terms with such service providers for the protection of Personal Information (known as data processing agreements or "DPAs") and that Apex performs adequate due diligence and monitoring of such service providers to ensure they can, and continue to meet the requirements of applicable privacy laws and contractual obligations made by Apex to third parties.

Apex has developed a service provider privacy management procedure to satisfy these requirements that is managed through Apex's procurement and third-party risk management functions. The process ensures all service providers are reviewed to ensure they can meet expected privacy obligations as well as to determine if contracts require updates. Associates responsible for service provider relationships must accurately answer questions about Personal Information Processing.

2. Clients and Partners

Privacy review of clients and partners and ensuring appropriate contractual terms are in place occurs through the regular engagement of the Legal Department for client and partner relationships. Where Apex will process Personal Information on behalf of a client (such as for Apex Silver), Apex may be considered the "processor" under applicable privacy laws and may need to enter into a DPA or similar terms as a service provider for that client.

3. Regulatory Requests and Subpoenas

Apex may also receive requests for Personal Information from regulators, such as SEC, FINRA, IRS, NFA, CFTC or other government agencies. All regulatory inquiries must follow Apex's Regulatory Inquiry Response Procedures available on the intranet. The Privacy Office works in collaboration with the Reg Requests Team regarding any regulatory requests regarding privacy matters.

Section 7: Data Protection Impact Assessments

Apex is required to conduct a data protection impact assessment (or privacy impact assessment) (“**DPIA**”) where processing Personal Information is likely to result in a high risk to the rights and freedoms of an individual subject to the Processing. The Privacy Office may also decide to conduct a DPIA in its discretion where it is appropriate to do so.

Non-exhaustive examples of when a DPIA may be required include:

- Processing biometric information, such as fingerprints, retinal images, facial scans.
- Processing special categories of information (or Sensitive Personal Information), such as geolocation data, racial/ethnic origins, political opinions, religious opinions, trade union status etc.
- Processing Personal Information of individuals under the age of 16 or of elderly or particularly vulnerable individuals
- Processing Personal Information for the purposes of profiling or evaluation of individuals, including profiling performance at work, economic or financial situation, etc.
- Ingesting any Personal Information into any artificial intelligence or machine learning engine or system, neural network, or similar system

Apex’s Privacy Office has developed a process to perform a DPIA to identify and minimize potential privacy risks to an individual in satisfaction of Apex’s legal requirements to perform a DPIA and industry best practices. Prior to commencing a new processing activity which may require a DPIA, Associates are required to contact the Privacy Office at privacy@apexfintechsolutions.com for an evaluation of whether a DPIA is required.

When a DPIA is required, employees must assist the Privacy Office in conducting complete and accurate DPIAs in a timely manner. When a DPIA is required, employees must receive approval from the Privacy Office prior to onboarding the new vendor and/or processing activity.

Section 8: Privacy Principles

Apex is required to adhere to certain privacy principles under privacy laws and industry best practices which guide how Personal Information should be handled and processed.

- 1. Lawfulness, Fairness and Transparency:** Apex must only process Personal Information if it has a lawful reason to do so under applicable privacy laws (*Lawfulness*), if individuals would reasonably expect the processing to occur (*Fairness*), and if Apex has provided adequate notice to individuals about the processing (*Transparency*). The Privacy Office has

determined through the ROPA where processing is lawful and fair and communicates this through Apex's privacy notices.

2. Purpose Limitation: Apex must only process Personal Information for purposes which are legitimate, in line with reasonable expectations of the individual and in compliance with any contractual obligations tied to the Personal Information under. This means that Personal Information can only be used for the purposes that it was originally collected for. The purposes that Apex may process Personal Information for can be found in our externally facing privacy notices, but include:

- Authenticating an individual's identity
- Processing requests and transactions
- Assisting and providing services to the respective client, correspondent or individual customer
- Managing fraud and security risk
- Responding to regulatory requests or privacy rights requests
- Incident management, response, investigation and remediation

Any department or team wishing to process Personal Information for a new reason or secondary purpose (such as for a new product or service), must contact the Privacy Office at privacy@apexfintechsolutions.com to determine if this is possible and to evaluate any potential privacy impacts, such as updates to relevant privacy notices and the ROPA and/or if a DPIA is required.

3. Data Minimization & Accuracy: Apex must ensure that it only collects and processes Personal Information that is adequate, relevant and limited to what is necessary for the relevant purpose. This means that Apex must not collect and process Personal Information if the same purpose or outcome can be achieved without collecting or processing that Personal Information. Apex must **not** collect more Personal Information than needed just because it may turn out to be useful later. Additionally, it is important that Apex makes sure that the Personal Information it maintains is accurate and, where necessary, kept up to date.

4. Storage Limitation: Apex must maintain Personal Information for only as long as required for the particular purpose of processing or for as long as Apex otherwise has a legitimate business need to maintain it (such as retaining the information under regulatory requirements or for defending litigation). In line with the *Purpose Limitation*, when Personal Information is retained for a particular purpose, it may only be processed for that purpose.

5. Integrity & Confidentiality: Apex must implement appropriate technical and organizational measures to ensure that Personal Information is appropriately secure and protected against unauthorized or unlawful processing and accidental loss, destruction or damage. Apex has implemented various security measures which are managed by the Apex Information Security Team.

Apex has also developed and implemented comprehensive incident response procedures enabling Apex to document, remediate and report any security or privacy incidents as required by Privacy Laws. Please see *Section 11: Reporting a Privacy or Security Incident* for further information.

6. **Accountability:** Apex must be able to demonstrate its compliance with this Policy, privacy laws and contractual obligations. Apex must ensure that privacy issues have been considered from an early stage in implementing services and procedures (*privacy by design*), and that, by default, only the minimum amount of Personal Information necessary is being processed (*privacy by default*). Apex does this by maintaining its Personal Information inventory and ROPA, by conducting DPIAs and other procedures.

Section 9: Protection of Personal Information

Personal Information is subject to Apex information security and other policies and procedures. In addition to those policies and procedures, all Associates are specifically required to exercise diligence and care whenever handling, using or processing Personal Information. The higher the sensitivity of Personal Information is being processed, the greater the protection, diligence and care that should be exercised (see Section 2: Personal Information for context on sensitivity).

1. **Internal Use.** In performing their roles for Apex (and regardless of access entitlements), Associates must use and share the *least* amount of and *lowest level of sensitivity of* Personal Information reasonably necessary to perform their job functions. For example:
 - Associates must not obtain and use a greater volume Personal Information than they need to perform a task; and
 - Associates must remove, truncate or mask identifiers, and other Personal Information fields from a dataset where they are not needed.

Associates must never leave Personal Information unattended at a person's desk or unlocked computer screen. If an Associate leaves his/her work area for any reason, their computer must be locked.

2. **Disclosure.** When sharing or disclosing any Personal Information (internally or externally), Associates must ensure that the recipient is authorized to receive all of the Personal Information being disclosed and no more Personal Information is being disclosed than is necessary for the purpose.

Personal Information can only be shared or disclosed through mechanisms or technology approved by Apex Information Security. The level of security required for a disclosure depends on the level of sensitivity of Personal Information. The more sensitive the Personal Information, the more protective the security controls and measures must be.

- 3. Storage.** Except for Incidental Processing, Personal Information should not be downloaded to local storage on any devices, including Apex issued devices. If an Associate has an urgent need to download Personal Information, Associates should download the Personal Information to a restricted folder in Apex's approved cloud storage solution or shared drive (for example, a folder only you have access to in an Apex cloud or shared storage drive).
- 4. Printing.** Associates may print Personal Information on approved Apex office printers when there is a legitimate business reason to do so but must immediately retrieve any printed materials that contain Personal Information. Associates are prohibited from printing any Sensitive Personal Information.
- 5. Personal Devices.** Personal Information is forbidden from being downloaded or sent to personal workstations, mobile devices (laptops, mobile phones, tablets, or removable media), or to systems outside of Apex unless in accordance with Apex's mobile device management policies and procedures.
- 6. Disposal.** After the expiry of a retention period or when there is no longer a legitimate business need to retain Personal Information, Personal Information must be properly destroyed or completely anonymized so that there is no reasonable way that any individual could be reidentified from it. Disposal procedures include:
 - Paper information must be shredded so that it cannot be practically read or reconstructed. Each Apex office has designated secure shredding bins.
 - Electronic information will be destroyed or erased so the information cannot be practically read or reconstructed.

In respect of any Personal Information stored or Processed by a service provider, Apex must ensure that Personal Information is promptly and securely disposed of at the termination of services or when the service provider no longer has a need for the Personal Information.

Further requirements regarding the security of Apex confidential information can be found in other policies and procedures, such as the Apex Information Security Policy.

Section 10: International Transfers

Data or information that is present in a country may be subject to the laws of that country. This could include data stored on servers, mobile devices or information in paper that is physically located in that country. Depending on the country and the data subject, this may pose a risk to rights and freedoms of the data subject due to lack of effective local data protection laws.

Under privacy laws, Apex is required to ensure that there is adequate protection in place for Personal Information when it is transferred from its origin country (i.e. the location country of the individual whose Personal Information is being transferred). Apex uses EU Standard Contractual Clauses and equivalent standard contractual clauses of other applicable jurisdictions in addition to adequacy decisions and performing transfer impact assessments to satisfy its privacy law obligation for international transfers.

Apex and its service Providers **may only** transfer Personal Information to, or permit access from, the following jurisdictions:

- Australia
- Brazil
- Canada
- European Economic Area (EU plus Iceland, Liechtenstein and Norway)
- Philippines
- South Korea
- United States
- United Kingdom

Transfers to Countries of Concern

Except to the extent that transfers are ordinarily incident to and part of the provision of financial services, Apex is prohibited from transferring any Customer Information relating to a US person to:

- (1) foreign entities headquartered in or organized under the laws of a country of concern;
- (2) foreign entities 50% or more owned by a country of concern or any of (1), (3) or (4);
- (3) foreign individuals primarily resident in a country of concern; and
- (4) foreign individuals who are employees or contractors of a (1) or (2) or a country-of-concern government.

Countries of concern as of the date of this Policy are:

- China (including Hong Kong and Macau)
- Cuba
- Iran
- North Korea
- Russia
- Venezuela

Please contact the Privacy Office to understand whether a particular transfer is ordinarily incident to and part of the provision of financial services.

Section 11: Privacy Awareness Training

Apex provides privacy awareness and security awareness training to all Associates at onboarding and on an annual basis. All Associates are required to complete this training when assigned by the due date.

Failure to comply with annual training requirements may subject Associates and others to revocation of access to Personal Information and/or disciplinary action up to and including termination.

At the time of hire, all Associates are required to sign and abide by the Apex employee agreements which also describes each employee's obligation to maintain confidentiality of information.

Section 12: Privacy Incidents

A privacy incident is an event that results in the unauthorized access, use, disclosure or acquisition of Personal Information. **Any Associate that becomes aware of a potential privacy incident must immediately report it to the Privacy Office (at privacy@apexfintechsolutions.com) and provide details of the potential incident to allow the Privacy Office to investigate it.**

Examples of privacy incidents include:

- Unauthorized access to a database containing Personal Information
- Accidental exposure of Personal Information to the public
- A laptop or mobile device being lost or stolen
- Emailing or sending Personal Information to the wrong recipient
- Personal Information not being properly destroyed or disposed of
- Sending Personal Information to a personal device or personal email account
- Publishing, using or sharing Personal Information when it has not been appropriately anonymized

The Privacy Office will investigate the potential privacy incident in coordination with the Legal Team and/or Information Security Team (where needed) and will escalate the potential incident to Apex incident response procedures if needed. Associates are required to respond promptly to requests for documentation and other information when the Privacy Office is investigating a potential privacy incident.

Section 13: Privacy Complaints

A privacy complaint is a formal expression of dissatisfaction by an individual (or another concerned party) regarding an organization's handling of their personal information under privacy laws.

Individuals have a right to lodge these complaints with regulators, and organizations, like Apex, must make individuals aware of this right. Apex makes individuals aware of this right where applicable under its externally facing privacy notices. Individuals may also lodge complaints directly with organizations like Apex.

Any Associate who receives or becomes aware of a privacy complaint directed at or concerning Apex must immediately escalate this to the Privacy Office and, if applicable, also follow the Apex Compliance Customer Complaint Policy.

Section 14: Artificial Intelligence

The processing of Personal Information by way of any artificial intelligence is prohibited under this Policy unless otherwise approved pursuant to other Apex policies or approved in writing by the Privacy Office.

Section 15: Contact Us

The Privacy Office at Apex is committed to supporting all departments and Associates in protecting Personal Information and compliance with Privacy Laws.

We encourage proactive engagement and are available to provide guidance, training, and consultation on all privacy matters. We can be contacted at privacy@apexfintechsolutions.com.

Policy Exceptions

This Policy applies a default position with respect to the protection of Personal Information across Apex combining a variety of legal, regulatory, contractual requirements and industry practices. The Privacy Office may grant limited exceptions to this Policy on a case-by-case basis in writing. To request an exemption, contact the Privacy Office.

Related Information

Document Name	Location
Apex Information Security Policy	Confluence
Cybersecurity Incident Response Plan	Confluence
Legal, Compliance and Enterprise Risk Incident Response Plan	Legal Department Shared Drive
Other Information Security Policies	Confluence
Apex Written Supervisory Procedures	Intranet
Apex AI Model Usage Policy	Intranet

Apex's Regulatory Inquiry Response Procedures	Intranet
APEX Third Party Risk Management Policy	Intranet
Customer Complaints Policy	Intranet

Policy Review and Approval

The Privacy Office is responsible for managing and updating this Policy. The Privacy Office will notify you via firm communications when updates to this Policy are made and require your review. This Policy can otherwise be found on the Apex intranet.

Revision History

Date	Version	Approver	Description of Updates
9/12/2025	1.0	Richard Stoneham	Finalized first version of the policy.

Appendix A – Personal Information

This appendix provides a deeper breakdown of what Personal Information and Sensitive Personal Information is with more examples. Whether a dataset contains Personal Information often comes down to a case-by-case analysis depending on the data, context and user permissions. This document aims to assist associates in identifying Personal Information, but should you have any questions please consult the Privacy Office at privacy@apexfintechsolutions.com.

CATEGORY	DESCRIPTION	EXAMPLES
Personal Information (“PI”) Other terms: • PII • NPI • Personal data	Definition: <i>Any information that relates to an identified or identifiable individual or (residential) household.</i> <u>What does “any information” mean?</u> Any information regardless of the format, medium or location can be Personal Information. This could be on a server, on paper, written onto a napkin or even carved into a potato. Information is Personal Information only if it relates to an individual. Information about a corporation, company, institution, club, trade union or other non-individual entities or groups of individuals is not Personal Information. However, information relating to an employee or other individual of these bodies or groups is Personal Information. <u>What does “relates to” mean?</u> This means there must be some form of link between the information and an individual. For example: • An account number for a corporation will not be Personal Information as it does not relate to an individual.	Common examples of data elements that alone constitute Personal Information (“identifiers”): a) Name (at least initial + last name) b) Username or account name c) Email address (personal or work) d) Residential address e) Phone number of an individual f) Account number or other unique identifier (including Apex Account Number or GUID²) g) Online identifier for an individual (e.g. social media handle) h) Device identifier (e.g. IMEI/MEID, or ICCID) for an individual’s personal or work device i) Internet protocol address (static or dynamic) j) Photographs, audio or video recordings of an individual k) Sensitive Personal Information (see below)

² A GUID is low sensitivity Personal Information under some laws (LGPD, GDPR, UK GDPR and in some other international jurisdictions), but will likely not be considered Personal Information under US law if the ability to link the GUID to an Account Number or other more direct identifier is tightly controlled

	• A ZIP code alone will not be Personal Information as it relates to multiple individuals or households, unless there is only one household in the ZIP code. <u>What does “identified” or “identifiable” mean?</u> An individual is ‘identified’ or ‘identifiable’ if they can be distinguished from a group of other individuals. Name is a common method of direct identification, but an individual can be distinguished from others by an identifier, such as an account number or unique ID. When considering if an individual is identifiable, you must also factor in all of the tools and other data sources available to the user or recipient. For example, could someone use the internet, generative AI or an application in combination with the data you have to identify someone? An individual can also be identified indirectly through combining data elements within a dataset (e.g. ZIP code + house color + car type); and/or by context or combining data with readily available information to the recipient. For example: a) A combination of data elements within the dataset (e.g. Apex Legal team member + Chicago office + blonde hair); and/or b) Context, information the recipient already has or tools available to the recipient to analyze the dataset¹.	Partial elements of the above in combination with other information can also be Personal Information. E.g. ZIP code + Last Name. Where Personal Information exists in a dataset, all information connected to each identifiable individual is also Personal Information. For example, where a spreadsheet separates individuals in rows by name, typically all information in that row relates to that individual. Context is important for establishing this. Here are some examples: • Transactions and account history • Investment suitability criteria • Physical and behavioral characteristics • Professional or employment related information • Marital status • Military or veteran status • National origin or citizenship • Facts or inferences or behaviors about the individual’s preferences, characteristics, trends, behaviors, attitudes, abilities or other attributes • Educational information • Professional or employment related information
--	---	--

¹ In 2000 it was shown that 87% of the US population could be identified using just 5-digit ZIP, gender and date of birth. (L. Sweeney, Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. [Here](#)).

		• Internet or search or browsing history • Sensitive Personal Information (below)
--	--	--

CATEGORY	DESCRIPTION	EXAMPLES
Sensitive Personal Information ("SPI")	Any Personal Information that: <i>a) is identified as requiring extra protection and control under privacy laws; or</i> <i>b) if it was acquired or accessed by an unauthorized third party could create a reasonable likely risk of substantial harm or inconvenience to the individual identified.</i> Sensitive Personal Information is a subcategory of Personal Information which is regarded as highly sensitive under privacy laws. Privacy laws have enhanced requirements for this category of information, including tighter use restrictions and stricter security controls. Apex's definition of Sensitive Personal Information encompasses the following privacy law definitions: • GDPR and LGPD: "special categories of data" • UK GDPR: "sensitive personal data" • CCPA: "sensitive personal information" • Regulation S-P: "sensitive customer information" • State breach laws: various terms	a) Government issued ID numbers (such as a social security, driver's license, state identification card, alien, tax or passport number); b) Government issued photo IDs (such as a copy of a passport, driving license or other photo ID) c) Any combination of information that can enable access to a consumer's account (regardless of multifactor authentication). For example: i) username, email address, account number, card PAN or ACH information; AND ii) any required security code or password to access the account d) Precise geolocation data that is accurate to within 1850 ft e) Personal information revealing citizenship or immigration status f) Personal information revealing racial or ethnic origins g) Personal information revealing political opinions h) Personal information revealing religious or philosophical beliefs

		i) Personal information trade union membership j) Data concerning health k) Genetic or neural data (DNA or data generated through measuring activity of an individual's nervous system) l) Biometric data (e.g. fingerprints or facial recognition scanning) m) Data concerning sex life n) Data concerning sexual orientation o) Criminal records or data revealing criminal history p) Any combination of Personal Information that if it was acquired or accessed by an unauthorized third party could create a reasonable likely risk of substantial harm or inconvenience to the individual identified.
--	--	--