Apporto

DATA PROTECTION POLICIES

(v. 1.3 – released 05/14/2025)

www.apporto.com

The herein-contained *Data Protection Policies* describe the rules and guidelines to be followed by all Apporto personnel regarding: minimum ("least-privileged") access, data handling, rotation of API keys, and back-up.

Any employee, temporary worker, contractor, or vendor found to have violated these policies may be subject to disciplinary action, up to and including termination of employment / contract / assignment, as well as, if applicable, civil action or criminal prosecution.

TABLE OF CONTENTS

INTRODUCTION

1. Overview

In the course of Apporto's provision of service to its clients, there is a need for the gathering and use of certain information. This information—collectively referred to herein as "protected data"—can include, but is not limited to:

- Personal data regarding individuals*
- Confidential information regarding corporations and other business entities

* "Individuals" can include customers, suppliers, business contacts, employees, and other people with whom the organization has a relationship or may need to contact.

Generally, "protected data" includes any and all information which is not otherwise accessible by the general public.

These *Data Protection Policies* describe how the aforementioned protected data must be: minimally accessed, collected, handled, and stored to meet the company's data protection standards, as well as to comply with the law.

2. Purpose

The overarching purpose of these *Data Protection Policies* is to protect Apporto—and thus Apporto's clients—from very real data security risks, including:

- ➢ Breaches of confidentiality
- ➢ Failing to offer choice (i.e., all clients/individuals should be free to choose how Apporto uses their data)
- ➢ Reputational damage (i.e.., damage suffered if hackers successfully gain access to sensitive data)

It is our policy to ensure that Apporto:

- ➢ Complies with applicable data protection law
- ➢ Follows current best business practices
- ➢ Is transparent as to how protected data is stored and processed

- Protects itself—and thus, its customers—from the risks of a data breach

3. Applicable Law

A. Data Protection Act

The Data Protection Act 1998 describes how organizations, including Apporto, must collect, handle, and store protected data.

To comply with the law, protected data must be collected and used fairly, stored safely, and not disclosed unlawfully.

The Data Protection Act is underpinned by important principles. These provide that protected data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant, and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Be processed in accordance with the rights of data subjects
- Be protected in appropriate ways

B. HIPAA

When Apporto accesses/stores data which is protected by HIPAA (Health Insurance Portability and Accountability Act), Apporto too must comply with HIPAA.

In regard to any such aforementioned protected data, Apporto adheres to the appropriate guidelines on electronic protected health information (ePHI) as issued by the U.S. Department of Health and Human Services (HHS). Specifically, Apporto complies with the applicable standards and implementation specifications of HIPAA's Security Rule with respect to ePHI.

Apporto implements controls to limit the access to information systems that maintain customer ePHI. Via internal controls, Apporto assures only

authorized access to the administrative tools that manage the resources critical to the operation of our information systems. Apporto further observes HIPAA's Privacy Rule and only uses or discloses ePHI as permitted by the Rule and the MSA in effect with the customer.

In addition, Apporto executes a *HIPAA Business Associates Agreement* with clients when applicable/required, setting out both Apporto's and the client's ("covered entity"'s) responsibilities, obligations, and restrictions.

C. FERPA

In compliance with FERPA (Family Educational Rights & Privacy Act), Apporto minimizes the PII (personal identifiable information) footprint to only student email, name, and possibly student ID (direct identifiers).

Apporto does not access or store any other direct identifiers, and no indirect identifiers. For the PII data Apporto does collect, all information is stored securely and only accessible based on role access to the data. For instance, only faculty members who teach courses in which the students are actually enrolled will have access to those students' PII. Only administrative roles have access to all users.

4. Scope

Apporto's *Data Protection Policies* apply to every individual working for, with, or on behalf of Apporto. This includes, but is not limited to:

- Apporto's headquarters (including all levels of management)
- All departments within Apporto
- All locations where Apporto does business
- All staff and volunteers of Apporto
- All contractors, suppliers, and other people working on behalf of Apporto

All data that Apporto accesses and/or holds relating both to identifiable individuals as well corporations/business entities is considered to be *protected data* and thus subject to these policies.

RESPONSIBILITIES

Everyone who works for or with Apporto has responsibility for ensuring that data is collected, stored, and handled appropriately. However, data protection is a key responsibility for certain personnel.

Regardless, each individual and/or team that accesses protected data must ensure that it is handled and processed in line with these policies and current data protection best practices.

1. General Staff

Apporto provides security and data protection training for all employees to educate them as to their responsibilities when handling data. Completion of cybersecurity training is required for all new employees, and annually thereafter. (See Apporto's *Policy on Policies* for more details.)

The only Apporto staff accessing data as covered by these *Data Protection Policies* should be those who have a *need* to do so for their work. (See *Minimum Access Policy* herein at p. 11 for more details.)

Employees should keep all data secure by taking sensible precautions and following the guidelines below:

- Data should never be shared informally. When access to protected data is required, employees can request it from their line managers.
- Strong passwords must be used, and they should never be shared. (For more information, see Apporto's *Password Policy*.)
- Protected data should never be disclosed to unauthorized persons, either within the company or externally.
- Data should be regularly reviewed and, if found to be out-of-date, it should be updated. If data is no longer required, it should be deleted and disposed of in a safe manner.

If an employee is ever unsure about any aspect of data protection, they should immediately request help from their manager or the Data Protection Officer.

2. Key Data Protection Personnel

Despite the company-wide responsibility for data protection, the following persons/departments have key areas of responsibility, as described below:

A. Data Protection Lead

Apporto's Data Protection Lead has key responsibility for the following:

- Reviewing all data protection procedures and related policies, in compliance with an agreed-upon schedule
- Arranging data protection training for those subject to these policies
- Handling data protection questions from personnel and anyone else subject to these policies
- Dealing with subject access requests (addressed herein at p. 29)
- Reviewing (and approving or declining) any contracts or agreements with third parties that may handle Apporto's protected data
- Keeping Apporto's Board of Directors updated regarding data protection responsibilities, risks, and issues

B. IT Manager

Apporto's IT Manager is responsible for:

- Ensuring all systems, services, and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure that security hardware and software is functioning properly
- Evaluating any third-party services that Apporto is considering using to store or process data—e.g., cloud-computing services

C. Marketing Manager

Apporto's Marketing Manager is responsible for:

- Approving any data protection statements attached to communications (such as emails and letters)
- Addressing any data protection queries from journalists or media outlets (such as newspapers)
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

D. Executive Management Team

Apporto's Executive Management Team bears the ultimate responsibility for ensuring that Apporto meets its legal obligations.

MINIMUM ACCESS POLICY

Apporto employs the principle of "least privilege" (also known as "minimal privilege" or "least authority") which restricts the access of every process, program, or user to (a) information required to meet a legitimate business need, and (b) with the least amount of access/information possible.

1. Rationale

The purpose of this *Minimum Access Policy* is to minimize the level of access which Apporto employees (including contractors, volunteers, and/or any other entities working for or on behalf of Apporto) have to files and directories which may contain protected data.

Implementation of this policy is intended to provide the following benefits:

- Reduce the avenues for cyber attacks that rely on the exploitation of privileged credentials
- Slow the spread of malware should a user's device become infected
- Improve system stability and operability because applications running with restricted rights have less ability to negatively impact the entire system and are therefore less likely to crash the system
- Streamline compliance audits through demonstrating compliance with a full audit trail of privileged activities

2. Provisions

Following are the specific provisions which Apporto utilizes in administering this *Minimum Access Policy*:

- Apporto's default position is to provide minimum access to files and directories based on the need to access them. As such, no unauthorized user should attempt to access files of a sensitive nature if presented with a password- or profile-restricted notification.
- Apporto administrators and users should leverage the "least privilege" practice by assigning permissions that meet the minimum data access requirements.

- In order to connect to Apporto's network resources, users must connect via authorized remote access gateways (RDP and/or SSH) with multi-factor authentication (MFA) to assure identity.
- Apporto users with privileged access should use non-privileged access/accounts when accessing non-sensitive information.
- Apporto audits users' level of access to determine if the current level of access is commensurate with current job requirements and to avoid "privilege creep."
- Administrators should consider temporary privileged access (a.k.a. "just-in-time" access) for situations where staff only require privileged access for a particular task or assignment.

USER ACCESS POLICY

Apporto manages users' access to its platforms and networks via its *User Access Form* which is administered and tracked via Jira ticketing system. The Jira form provides an auditable trail that can be easily and quickly referenced to activate, modify, and/or deactivate a user's access.

Based on the provisions and instructions below, the *User Access Form* is designed to ensure that:

- Requests are properly reviewed and approved
- Access is granted based on the user's role and responsibilities
- Changes to access requests are tracked and approved
- Incidents related to access requests are identified and addressed

1. Provisions

The purpose of this *User Access Policy* is to ensure that users have the level of access required to perform their job and that their access is approved by the appropriate personnel authorized to do so.

These instructions also provide standardized levels of access for each job or family of jobs within the Company.

To effectively manage access, this policy and the accompanying *User Access Form* have the following provisions/restrictions:

A. Segregation of Duties

- ➢ No single role can both initiate and approve access requests.
- ➢ A separate approving manager should be designated for each access request.

B. Access Controls

- ➢ Each request is reviewed and approved by the authorized personnel set out in these instructions.

- For tracking and auditing purposes, a unique authorization code will be assigned to each request in Jira.

C. Change Management

- Modifications to a user's level of access must include the reason for the change, the effective date, and specify the duration of the access.
- Modifications to a user's level of access should be approved by the same approving manager that approved the original request.

D. Monitoring

Access requests should be tracked to include:

- Status of the request (i.e., *Initiated*, *Under Review*, *Approved*/*Denied*
- Date of approval
- Date access is granted
- Date access is terminated

The queue of access requests and their status is reviewed periodically by Apporto's Security Team to detect and prevent unauthorized access. The Security Team also performs periodic reviews of users' levels of access to verify the level of access is appropriate to the users' job requirements.

E. Incident Management

If, during the process of reviewing access requests, an approving manager believes the request is an attempt to gain unauthorized access or is any way suspicious, it should be notated as such on the form and forwarded to Apporto's Security Team. The Security Team will treat these situations as a possible security incident and will investigate it accordingly.

Based on the receipt of any such incident reports, the Security Team will make recommendations to the Executive Team to identify and address any perceived weaknesses in the access request process.

2. Designated Approving Managers

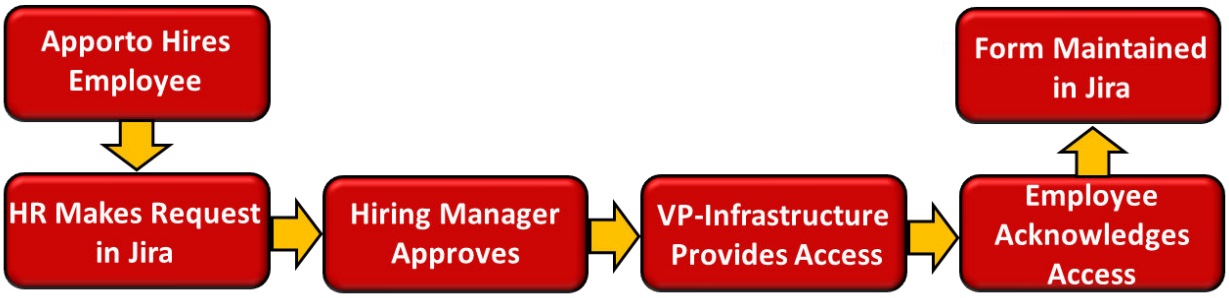
The following roles are designated to review and approve access requests for their respective teams:

Team	*Approving Manager*
Infrastructure	VP of Infrastructure
QA	VP of QA

3. Instructions

Apporto's *User Access Form* is maintained in Jira. For new hires, Apporto's Manager of Human Resources initiates the process and completes the form for minimum access. Once an employee receives minimum access privileges, the employee can then make requests in Jira for expanded access. If an employee does not have Jira access, their manager will make the request in Jira.

User access requests consist of a multi-handoff review and approval process. The workflow for new-hire user access requests is indicated in the graphic below:



To correctly complete the *User Access Form*, the following information is required.

A. User Information

1. Full name
2. Job title

3. Department or team
4. Email address
5. Phone number

B. Access Request

1. Type of request: Activation, Modification, Deactivation
    a. Activation: This is for new users only, i.e., those without any current access to any of Apporto's network, platforms, applications, etc.
    b. Modification: If you currently have any level of access and wish to modify it, e.g., gain access to a new application, change level of access, terminate current access, etc., choose this selection.
    c. Deactivation: This is used when a user is terminating all access to Apporto's network, platforms, applications, etc., typically at termination of employment
2. If modifying or deactivating a request, provide a list of all of your current access and level of access if applicable.
3. System/application name for which access is requested
4. Level of access requested
5. Reason for access
6. Duration of access

C. Authorization

1. Approving manager's name
2. Approving manager's title
3. Security Team review
    a. If the approving manager wishes Apporto's Security Team to review the request, check "Yes" and forward to the Security Team.

4. Date approval granted
5. Date access to begin
6. Date access is to terminate
7. Authorization code

D. Security Team Review

If the approving manager requests a Security Team Review, this section will be completed by Apporto's Security Team.

1. Has the user experienced any previous security-related issues?
2. If "Yes," the Security Team is to provide a brief explanation and include the date(s) of the incident.
3. Is the user's request recommended?
4. If "No," the Security Team is to provide a brief explanation.

4. Deactivation of Access

User access will be deactivated upon the following conditions:

1. User no longer has need for their particular level of access
2. User terminates employment with Apporto
3. User's account is compromised in a cybersecurity incident

DATA HANDLING POLICY

1. Data Separation & Encryption

Apporto offers two (2) options for cloud services: multi-tenant cloud and dedicated cloud. Each Apporto multi-tenant customer receives their own partitioned environment with all data logically and physically separated at the virtual machine (VM) level. Certain resources, such as streaming servers, web servers, VPC, active directory servers, and VPN routers, may be shared between customers, but strict measures are in place to isolate user information and access between customers.

In contrast, dedicated cloud services provide customers with exclusive access to all resources, including those mentioned above.

Regardless of the cloud option chosen, customer data, such as user profiles and databases, are encrypted at all stages of access. Data-at-rest encryption is used to secure VMs that hold user profiles, as well as database back-ups. Access protocols are configured to allow only authorized access, and encryption in the protocol is utilized at the highest level possible for interoperability.

Users can only access their data through public Apporto services via encrypted protocols such as SSL/TLS (HTTPS, SFTP, etc.) to ensure the confidentiality and integrity of their data.

All public-facing websites will utilize the latest encryption that is widely accepted as secure and interoperable (currently TLSv1.2 is the highest supported version). All SSL certificates will be up-to-date and issued from respected CAs (Certificate Authorities).

Cryptographic key management will be used to protect encryption keys. The specific key management solution will be provided by our Cloud Vendor's IaaS key management solution.

All public-facing websites will be encrypted with at least 2048-bit certificates from a trusted CA.

2. Data Storage

Apporto uses cloud infrastructure for all of its needs. Therefore, we have no policy around physical media handling, and instead rely on our data-at-rest encryption and the cloud vendor's data protection agreements to mitigate the risks associated with the lifecycle of physical media.

When data is stored, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts.

- Data should be protected by strong passwords as governed by Apporto's *Password Policy*.)
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud-computing service.
- Data should never be saved directly to laptops or other mobile devices (such as smartphones or tablets).
- Servers containing protected data should be sited in a physically secure location where only authorized personnel have access.
- Data should be backed up frequently; those back-ups should be tested regularly, in compliance with Apporto's *back-up Policy* contained herein.
- All servers and computers containing data should be protected by approved security software and a firewall.

Any/all questions about storing data safely should be directed to Apporto's Data Protection Officer or IT Manager.

3. Data Back-up

Back-ups are automatically performed on system-specific schedules, and back-up results are stored in secure, encrypted format. The schedules are documented internally at the vendor.

All back-ups will be shipped digitally to an offsite back-up site for disaster-recovery purposes.

Data back-ups will be employed at Apporto to protect both Apporto's and customer's data. A customer can request a data export of their recently backed-up data. Back-ups are stored based on the roll-over requirements for the back-ups. Roll-over requirements vary by data type and change frequency.

At the conclusion of a customer's contract, their data will be returned or destroyed per the terms of the Master Service/Subscription Agreement (MSA) (and/or the HIPAA Business Associate Agreement, if applicable).

For more information regarding Apporto's back-up policies, see the *Back-up Policy* contained herein.

4. Data Use

Protected data is of no value to Apporto unless the business can make use of it. However, it is when protected data is accessed and used that it can be at the greatest risk of loss, corruption, or theft.

- When working with protected data, employees should ensure the screens of their computers are always locked when left unattended.
- Protected data should never be shared informally. Protected data should never be sent via email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The Data Protection Officer and/or IT Manager can explain how to send data to authorized external contacts.
- Employees should never save copies of protected data to their own computers. Always access and update the central copy of any data.

Ownership rights of data, inputs, outputs, and metadata is maintained by the customer. This policy is documented at https://apporto.com/privacy.

5. Data Accuracy

The Data Protection Act requires that Apporto take reasonable steps to ensure that data is kept accurate and up to date. Therefore, it is the responsibility of *all* Apporto employees to take positive steps to ensure that

this occurs, i.e., that data is always kept as accurate and up-to-date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated—e.g., by confirming a customer's details when they call.
- Apporto will make it easy for data subjects to update the information Apporto holds about them (such as via the Apporto website).
- As inaccuracies are discovered, data should be updated. (For instance, if a customer can no longer be reached on their stored telephone number, that number should be removed from the database.)
- It is the Marketing Manager's responsibility to ensure that marketing databases are checked against industry suppression files every six (6) months.

API KEYS POLICY

1. Purpose

Rotating API keys is a widely accepted best practice for the security of our networks and platforms, assuring the security of our and our clients' sensitive information. It also makes tracking usage and detecting suspicious activity more efficient. Because Apporto rotates API keys, even if a key is compromised, data remains safe and secure.

2. Scope

This *API Keys Policy* applies to all applications used by Apporto which are protected by API keys.

3. Policy

A. Least-Privileged Access

Consistent with Apporto's *Minimum Access Policy* contained herein, the company also employs a least-privileged access approach to API keys. Only employees with a "need to know" role are given access to the API keys.

B. Keys Found in Code

Production API keys do not belong in code. If they are found in code:

1. They should be pulled out and placed in a configuration file.
2. The API key rotation process described below is followed.
3. QA performs additional testing to verify that the modified code remains functional.
4. After passing all QA tests, the code is sent to production for deployment.

C. Rotation Prompts

Similar to Apporto's *Password Policy*, Apporto only rotates API keys when there is a need to do so. Some examples of when such a need occurs are as follows:

- A data breach
- A key is somehow compromised
- An employee with API key knowledge/access leaves the employ of Apporto
- Keys found in code (see above)

D. Rotation Process

1. A new API key is created.
2. The new access key is introduced, and all applications are updated to use the new key.
3. Apporto's QA Team or SA Team validates that the new key/application is functioning correctly.
4. The previous key is set to "inactive."
5. The inactive key is deleted or archived.

E. Coordination

The rotation of API keys requires careful coordination to avoid any interruption of service. There are two (2) scenarios which may apply:

1. Both the sender and the verifier (or client and server) must have the new key and the keys are updated/rotated at the same time. This may occur during a maintenance window where there may be some downtime until all keys have been rotated.
2. In the case with hyperstream and the AppStore, there is the ability to update the keys dynamically as well as the ability to list multiple keys. What this allows Apporto to do is keep the configuration as is, but when keys are rotated, the new key is added to the configuration file, so that both the new and the old keys remain functional. Then the AppStore is configured to use the new key. Once all applications have been converted, the previous key will be removed.

BACK-UP POLICY

The goal of this *Back-up Policy* is to describe Apporto's back-up environment, the decisions that led to it, and the procedures for using the environment in sufficient detail so that, if necessary, an IT person with no knowledge of the unit will be able to perform essential back-up or recovery functions.

1. Back-up Configurations

A. Back-up System

All back-ups are performed using integrated cloud solutions: (a) AWS back-up for AWS Cloud VMs, and (b) Azure Recovery Services for Azure VMs.

B. Back-up Policies

The following back-up policies are configured based upon RTO* / RPO** of the target. Targets are then added to the matching policy type to enable back-ups. AWS Targets are added via tag **back-up:<policy>**. Azure targets are added with **Operation->back-up->Vault->Policy**.

* RTO = Recovery Time Objective (the maximum time that a service can be down after a disaster)

** RPO = Recovery Point Objective (the maximum age of data that can be lost due to a major incident)

i. Cloud (AWS/Azure) Back-up

Daily

Snapshot of tagged VMs run daily at 5 a.m. UTC. Retention of daily back-ups: for five (5) calendar days.

Weekly

Snapshot of tagged VMs run weekly every Sunday at 5 a.m. UTC. Retention of weekly back-ups to be retained for fourteen (14) calendar days.

Critical

Snapshot of tagged VMs run daily at 5 A.M. UTC, to be retained for five (5) calendar days. Retention of weekly back-ups to be retained for twenty-one (21) calendar days.

* Apporto has implemented a distributed file storage (DFS) solution on its domain controllers (DCs), with file server resources hosted on dedicated servers that are allocated to each customer (with more than 1TB planned storage).

ii. Profiles Back-up

Snapshot (so called SHADOW COPY) of users' profiles should be executed on an hourly basis, every hour. Retention is automatic with maximum storage of 100-150 GB.

iii. Web Databases Back-up

Back-ups of mysql or other critical databases run daily at 5 a.m. UTC. Retention of daily back-ups to be retained for fourteen (14) calendar days.

2. Back-up Procedures

A. Back-up Roles

Primary back-up administrator: Eduard Marchenko (eduard@apporto.com)

Secondary back-up administrator: Sergii Vinnikov (sergii@apporto.com)

B. Weekly Tasks

Every Monday, the back-up administrator reviews the status for the previous week's back-up activity to verify that all jobs were completed successfully. Any errors or unsuccessful jobs must be immediately investigated to determine the cause, and action must be immediately taken to complete unsuccessful jobs.

3. Back-up Policies Assignment

On a daily basis, as a pre-scheduled task, Apporto conducts a comprehensive review of all resources in use in both clouds. During this review, the script assigns tags to each resource based on its server name and role. The methodology entails examining the server name and extracting the role

information. Based on predefined mappings, the system then assigns appropriate tags to each resource, indicating its role or function within the infrastructure:

- All *-TEST and *-APP000 (golden images) VMs should have DAILY policy/tag assigned.
- All RDS1/GPU1 (primary) servers should have WEEKLY policy/tag assigned.
- All DC1 should have CRITICAL policy/tag assigned; all DC2 should have WEEKLY policy tag assigned.
- All DB servers should have DAILY policy/tag assigned.
- All GUAC/PROXY/CHR VMs should have WEEKLY policy/tag assigned.
- Every profile storage server (DC or FS) D drive should have SHADOW COPY configuration for profiles storage, every hour, 100-150 GB size, depending on disk size.

4. Cleanup/Rotation Procedures

Once per quarter, review for staled VMs and snapshots/back-ups and remove unused entries.

5. Full System Recovery Testing

At least once per year, the back-up administrators make a full restore of primary front-end web servers and databases to confirm/test functionality of systems after restoring and keep the *Disaster Recovery Plan* (DRP) consistent. All other systems have full redundancy configured with N+1 or N+2 levels.

Appendix A: Recovery/DR Test Log

Date	Test Target	Objects Recovered	Result	Elapsed Time	Test Performed By

Appendix B: Restoration of a Complete System

Step 1: Create test VPC

Step 2: Restore from full back-up latest version of DRUPAL server to new server (Azure feature)

Step 3: Restore DB into new instance (Azure feature)

Step 4: QA team tests functionality with “hosts” file modification

DISCLOSURE OF INFORMATION

1. Subject Access Requests

All individuals who are the subject of personal data held by Apporto are entitled to:

- Ask what information Apporto holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how Apporto is meeting its data-protection obligations

If an individual contacts Apporto requesting this information, this is called a *subject access request*.

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at itsec@apporto.com. The Data Protection Officer can supply a standard request form, although individuals do not have to use this.

Of course, the Data Protection Officer will always verify the identity of anyone making a subject access request before handing over any information.

NOTE: Individuals will be charged $10 USD per subject access request. The Data Protection Officer will aim to provide the requested data within fourteen (14) business days.

2. Other Disclosures

In certain circumstances, the Data Protection Act allows protected data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Apporto, as required by law, will disclose requested data. However, the Data Management Officer will ensure that the

request is legitimate and legal, seeking assistance from the Board of Directors and/or Apporto legal counsel where necessary.

3. Privacy Statement

Apporto aims to ensure that individuals are fully aware:

- That their data is being processed
- How their data is being used
- How to exercise their rights

To these ends, Apporto has a privacy statement setting out how protected data is used by the company. This is available upon request, and further is available on Apporto's website.

Document Review / Revision History

Date	Version	Action / Change	Reviewed / Approved By:
05.14.2025	1.3	Updated data back-up retention policy	Nahum Nicholas
06.26.2024	1.2	Addition of User Access Policy	Travis Markley
06.13.2023	1.1	Addition of API Keys Policy	Sergii Vinnikov
05.17.2023	1.0	Policy release	Sergii Vinnikov

Effective Date: 05.14.2025
Review Cadence: Annually
Next Scheduled Review: 05.14.2026