How we manage candidate and customer data

A summary of the data we collect and how we use, store, protect, and destroy it.

Version 2.0
20 July 2022

sapia.ai

Data Management at Sapia.ai

Executive Summary

As an AI business, Sapia.ai recognises the importance of data management, security, and transparency as to how we use, store and protect your data.

This document aims to help set out how we comply with our obligations and the rights of data subjects under Europe's General Data Protection Regulations (GDPR), the Australian Privacy Principles (APP), and equivalent data privacy legislation. By extension, the document outlines the technical and organizational controls we employ to deliver these obligations.

Personal Data provided to Sapia.ai by the candidate applying for employment with our customer, such as in response to the interview questions, is low risk. However, processing may sometimes include limited special categories of Personal Data.

Sapia.ai provides services in multiple regions. We use Amazon Web Services (AWS) to process and store Personal Data. All AWS services are hosted within our customer-chosen AWS Data Centre, typically located in your sovereign location.

The number of individuals affected by data collection and processing varies in each situation as it is representative of the volume of applications for a job role.

This document should be read in conjunction with the Sapia.ai Privacy Policy.

Definitions used in this document

Customer Provided Data – data that you provide to us and can include data relating to your candidates and employees, for example, their name, phone number, email address, employment status, race, or gender.

De-identified Derived Data – this data results from taking Processed Data and/or Raw Data and using all best endeavors to remove all identifying information concerning candidates or third parties. De-identified Derived Data also includes further processed versions of the forgoing.

Interview Data – candidate responses to the structured interview questions and video responses.

Personal Data – any information relating to an identified or identifiable natural person or any such definition in data privacy legislation, for example the EU's General Data Protection Regulation.

Personally Identifiable Information (PII) – identifiable data such as first name, last name, email, contact number, location, or IP address.

Processed Data – this is data that is the output of Raw Data being processed for the customer by Sapia.ai. However, it may be possible to reverse map and "re-identify" a candidate against the Raw Data.

Raw Data – this is the unprocessed information (including text or videos) that we collect from you or from candidates.

Introduction and Overview

The purpose of this document is to give transparency and insight into data management at Sapia.ai.

Sapia.ai provides an online text-based assessment whereby candidates answer free-text or multiple-choice questions based on past experience, situational judgment, and values. Our proprietary personality, competency, and skill classifiers, powered by Natural Language Processing and Machine Learning, extract attributes from these answers. We then provide a score and corresponding recommendation for the candidate's suitability for the role.

Additionally, Sapia.ai offers a video interview platform that allows candidates to record an answer to a question (both audio and visual). We collect this and present it to our customer for review. Video responses are **not** subject to Ai analysis.

We typically integrate Sapia.ai with your existing tech stack, such as an Applicant Tracking System, or a standalone SaaS solution can be deployed. Each user of Sapia.ai systems will have a user account created in order to review or rate a candidate interview. This user account is either protected by Single Sign-On (SSO) or with a username and password, protected by Multi-Factor Authentication (MFA).

We recognise our responsibility to maintain the highest data privacy and security standards. Therefore, we ensure the security of your data in our software with encryption in transit and at rest. In addition, our application undergoes regular penetration testing and security reviews by white-hat security firms.

This document consists of the following sections:

1	Data Collection	The different types of data that are required to be collected to provide services to you
2	Data Purpose	Why your data is required
3	Data Processing, Storage & Sharing	Where and how your data is processed, stored, and shared
4	Data Protection	How we ensure your data is kept safe
5	Data Management & Destruction	How we de-identify and destroy your data

1 Data Collection

As a Data Processor, Sapia.ai collects the minimum data possible to provide the services to you.

We collect Personally Identifiable Information (PII) about candidates, including full name, email address, phone number, location, and IP address. This is collected from candidates directly through the web application experience or passed to us from your integrated application, such as your Applicant Tracking System (ATS).

When creating user accounts for employees of your organization, we will collect PII data about your employees, including name, company email, telephone number, and job title. You either provide this information to us manually, or the details are received via your Single Sign-On Identity Provider (IDP).

In addition, **and only if agreed by you**, we may collect candidate special category data (Demographic Data) which may include, but is not limited to, age, gender, race, and disability status. Again, this is collected from candidates through the web application experience or passed to us from your integrated ATS.

As part of our core offering, we collect candidate responses to the structured interview questions, along with video responses (Interview Data). This information is input manually by each candidate.

Like most other organizations, we may also collect information about how and when you or your candidates interact with our platform. For example, device type, browser version, where users click, scroll their mouse, or move between pages (Behavioral Data). We collect this information using third-party software and cookies, such as Hotjar or Heap. The only PII shared is the candidate or user IP address.

Our Customers share information with us, such as a list of candidates hired or rejected, churn, and performance data (Customer Provided Data). You choose how to send us this data, whether it be encrypted email, via file share software, or our preferred method, secure file transfer protocol (SFTP).

The data collected is detailed below:

Data	Description	Example(s)
Personally Identifiable Information (PII)	Information collected from candidates used to identify them during the recruitment process. This is provided manually by the candidate in our unintegrated solution or is provided by the ATS via API when integrated Information collected about your employees (users) to create an account to view and rate candidate interviews	Email address Name Phone number Location IP Address Name Email Phone number Job title

Demographic Data	Information to understand the demographics of your candidate pool (provided by the candidate) When not provided by the candidate, we use PII (name) to infer gender and ethnic origin. PII will not be stored with any anonymized data Sapia.ai creates and will always be kept separate	Age Gender Disability status Ethnicity English is a second language Aboriginal origin group
Interview Data	Responses to questions, testing for competencies in the interview process (Chat Interview) Audio and visual recording of responses to questions (Video Interview) Data representing the results of running the candidate responses against the model to test for applicability to the vacancy	Free text and multiple choice answers to questions in Chat Interview Answers to questions in Video Interview Predictions and supporting intermediate feature data
Behavioral Data	Browser and technical information to test for equivalence across different devices (i.e. desktop vs mobile) when candidates are completing an interview The behavioral information to gain a better understanding of how users interact with our product(s) and identify issues that users are running into when using such products.	The browser and device name & version. IP address to collect approximate location. Interactions (e.g., where users click, scroll their mouse, move in between pages). This is used to create visual representations of the experience.
Customer Provided Data	Data from the employer that feeds back to Sapia.ai to retrain the model and improve accuracy	Candidates hired and rejected or employees that were candidates that have resigned or been terminated, results of performance reviews for candidates that have become employees

2 Data Purpose

Personally Identifiable Information (PII) from your candidates is used to identify them in our platform and, when necessary, infer gender and ethnic origin from the name, allowing testing of our AI and predictive models for adverse impact.

PII about system users (your employees) is used to provide access to our web application (the "platform"), perform our obligations under the contract between us, and for certain marketing activity such as announcing new product features.

Demographic Data (i.e, gender, ethnicity, age, etc.) is only used for reporting and bias testing of the AI at an aggregate level or to improve or modify our product suite.

Interview Data is used to to evaluate a candidates capability with reference to a competency framework shaped by you. Sapia.ai then forms a picture of the candidate that can be used by you to assess them for the role and then coach and improve their performance in your organization.

Sapia.ai turns Interview Data captured in the chat interview product, along with PII and Demographic Data into De-identified Derived Data to build and maintain our predictive models and to create analytical and statistical data to improve, modify, or develop our products. We may also use this De-identified Derived Data to support published research in scientific journals. Data captured from the video interview product is excluded from this, therefore it is **not** subject to AI, is not transcribed, and is not retained beyond the customer agreed retention period.

Behavioral Data is collected to better understand how users interact with our product(s) and identify issues users are running into when using such products. It is also used to test for equivalence across different devices (i.e. desktop vs mobile) when candidates are completing an interview.

Customer Provided Data further helps us build and maintain predictive models or create analytical and statistical data.

We may also process Personal Data from your candidates or users (together, the "Data Subjects") to perform our contractual obligations to you, including to communicate with you and provide you with any relevant customer service; for billing and account services; for data analysis such as audits and fraud prevention; as required by applicable law; or to enforce our terms and conditions and to otherwise operate and support the Services.

Sapia.ai is set up to facilitate certain data subject rights, such as those described by the European Union, the United Kingdom, and Australia. We will take a sensitive (never a one size fits all/blanket) approach to work proactively with the candidate or user as well as its customers in facilitating these rights.

3 Data Processing, Storage & Sharing

Candidate recommendations, insights, and communications are formed through the processing and storage of data in Sapia.ai systems, hosted by AWS.

Sapia.ai has chosen Amazon Web Services (AWS) - the world's most comprehensive and broadly adopted cloud platform to help us build, maintain and grow a secure and scalable solution.

AWS is the most flexible and secure cloud computing environment available today. The core infrastructure is built to satisfy the security requirements of the military, global banks, and other high-sensitivity organisations. AWS's physical infrastructure has been accredited under ISO 27001, SOC 1/SOC 2/SSAE 16/ISAE 3402, PCI Level 1, FISMA Moderate, and Sarbanes-Oxley.

Data Sovereignty

The AWS cloud offering spans 25 geographic regions worldwide, each with multiple Availability Zones. In consultation with you, we can process and store candidate data in the AWS region **chosen by you**, for example, North America, Europe, or Asia Pacific, to maintain data sovereignty.

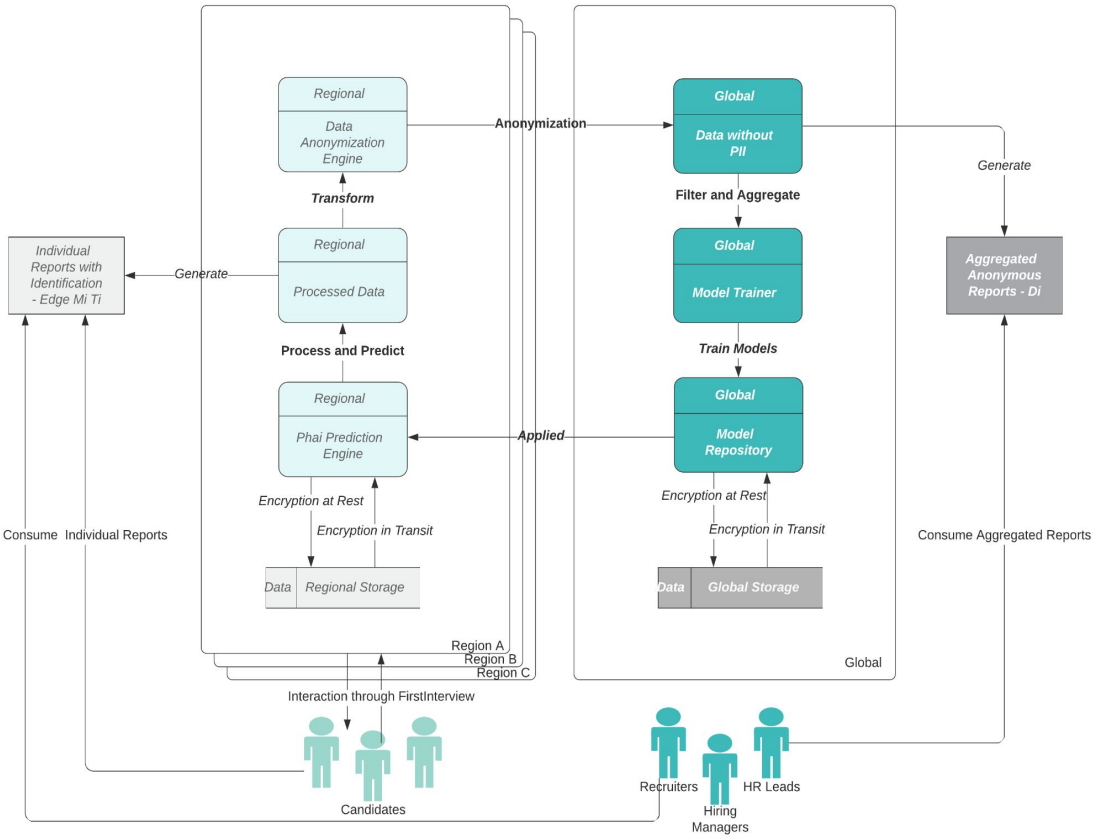
Regional Storage
Customers can choose the region where they like to store their data in. Typically, it will be the region nearest the customer's business location. For example, suppose a customer is located in the US. In that case, they may choose to store their data in the AWS US East (N. Virginia) region.

Raw Data submitted by candidates and Processed Data are all stored in their respective regions to show individual reports such as My Insights and Talent Insights.

Global Storage
We use a state-of-the-art anonymization algorithm to de-identify any Personally Identifiable Information in the record. We save De-identified Derived Data to a centralized location chosen by Sapia.ai. Currently, it is the AWS Asia-Pacific (Sydney) region.

De-identified Derived Data is stored in a central location for monitoring bias, building and improving models, and conducting organization-wide analyses and reports. Only using regional data for the above purposes might result in suboptimal performance or incomplete analytics results.

This is illustrated on the following page.



Processing of Data

The following AWS services are used by Sapia.ai to process the data collected:

Service	Description
AWS Sagemaker	Amazon SageMaker is a fully managed machine learning service
AWS Lambda	Lambda is a compute service that allows us to run code without provisioning or managing physical servers
AWS Elastic Container Service (ECS)	ECS is a container management service
AWS Simple Queue Service	Amazon Simple Queue Service (SQS) is a fully managed message queuing service that allows us to run serverless applications
AWS Pinpoint	Amazon Pinpoint is used to send push notifications, emails, and SMS text messages, and analyse user behavior

Any data processing by an individual Sapia.ai employee is achieved via AWS QuickSight or AWS WorkSpaces, a persistent desktop virtualization service deployed within an Amazon Virtual Private Cloud (VPC) in your selected region. No data is stored on the employees' local devices.

Customer Provided Data received manually (for example, via encrypted email) is added to the Amazon Cloud and deleted from local devices at the earliest opportunity.

Testing for bias
Sapia.ai also processes data to test for bias. We use an optimization algorithm to generate the final score for each candidate and execute bias testing. These are then used as a constraint within the optimization process to ensure the resulting model is not biased.

By default, we use gender (binary - male/female) and ethnic origin to set the bias constraints. The current ethnic origin groups are Asian, South Asian, European, African American, African, Latin American, Middle Eastern, and Pacifica.

In cases where we do not collect this demographic information from the candidates directly, we use our own proprietary algorithm (Name-py) to derive both gender and ethnic origin from the name.

If additional demographic parameters are available and voluntarily provided by the candidate, we can test for those, for example, English as a Second Language (EASL), Aboriginal and Torres Strait Islander people (First Nations) groups, age, and disability status.

Models are tested for bias on the individual, aggregated, and recommendation level. We test before model deployment and continually once the model is live. We also share anonymized stats on any known bias with our customers in our Discover Insights product, which runs on AWS QuickSight. In addition, we can provide custom reporting if more details are required.

Immediate corrective action is taken if bias is identified within the model.

Storage of Data

The following AWS services are used by Sapia.ai to store the data collected and processed:

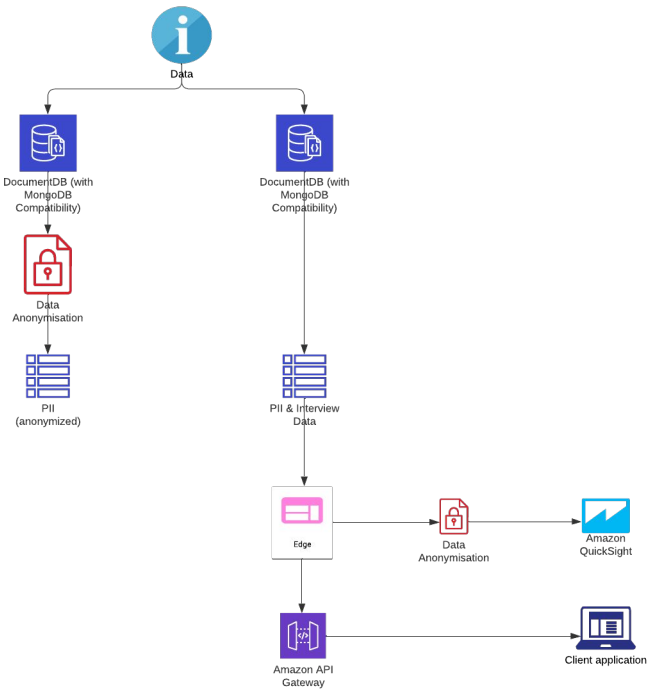
Service	Description
AWS S3	Amazon Simple Storage Service (Amazon S3) is storage for the Internet. Access control defines who can access objects and buckets within Amazon S3, and the type of access (for example, READ and WRITE). The authentication process verifies the identity of a user who is trying to access Amazon Web Services (AWS)
AWS DocumentDB	Amazon DocumentDB (with MongoDB compatibility) is a fast, reliable, and fully managed database service allowing us to set up, operate, and scale MongoDB-compatible databases in the cloud

AWS DynamoDB	Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability
AWS OpenSearch Service	Amazon OpenSearch provides a highly scalable system for providing fast access and response to large volumes of data with an integrated visualization tool
AWS Redshift	Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the AWS Cloud
AWS Kinesis	Amazon Kinesis powers Data Analytics for SQL Applications

Additionally, Personally Identifiable Information (PII) is duplicated, then de-identified, and stored separately in AWS DocumentDB. This enables us to build and maintain predictive models, create analytical and statistical data, and test for bias, all using De-identified Derived Data.

We de-identify the copy of PII using an open-source algorithm. All identifying information is encoded in a non-reversible format, for example *John Smith* may become *ef61579cbbd64cbcf7af8518eefb8e58cbe0b8cdac4a*. Reversing this data is mathematically and practically impossible.

The original PII is then stored alongside Interview Data during your retention period to allow you to identify each candidate within our platform, and identify which set of interview answers belong to which candidate.



World-Class Data Encryption

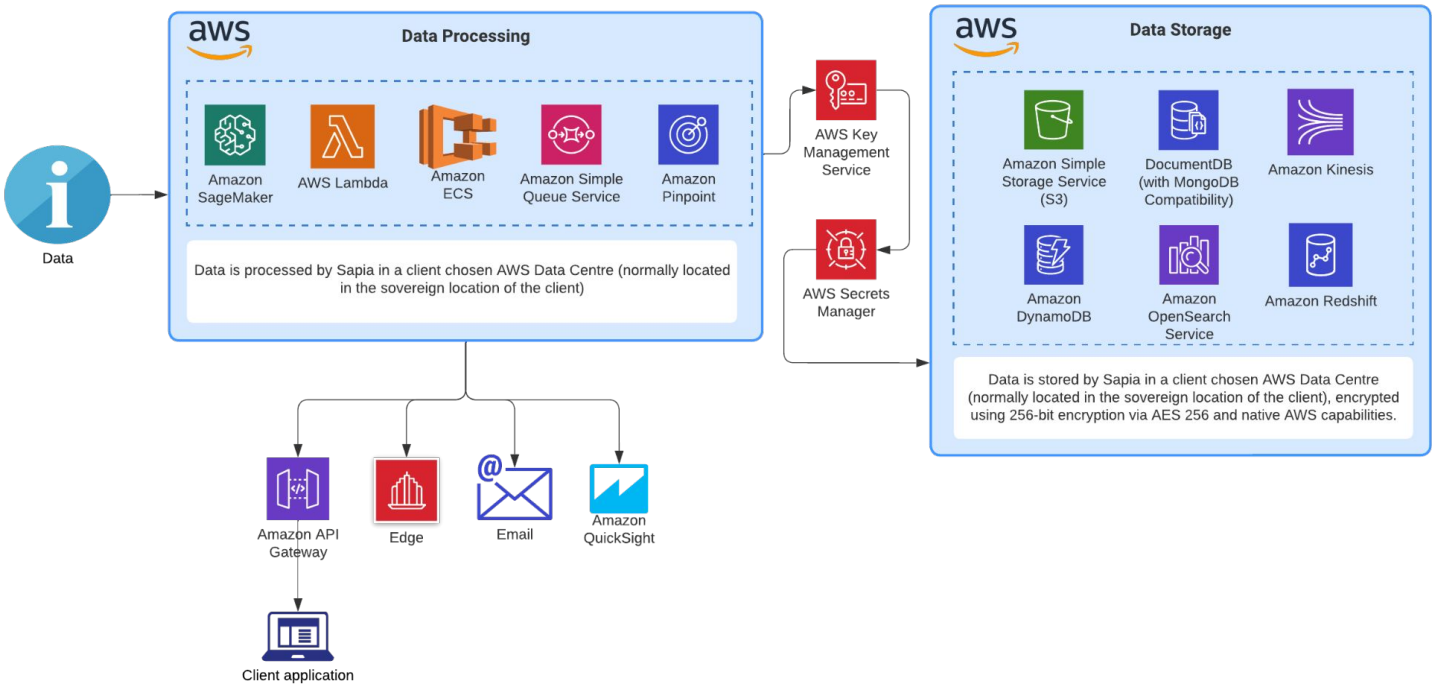
When data is stored, it is said to be 'at rest'. When data is being processed or transferred between the browser and the processing elements of the system, it is said to be 'in transit'.

Sapia.ai encrypts data-in-transit using bank-grade secure sockets layer (SSL) and Transport Layer Security (TLS) 1.3, the safest method available today. Data is encrypted at rest using 256-bit encryption via AES 256 and native AWS capabilities. Encryption keys are managed using the following AWS services:

Service	Description
AWS Key Management Service	AWS Key Management Service (AWS KMS) is an encryption and key management service scaled for the cloud
AWS Secrets Manager	AWS Secrets Manager allows us to securely encrypt, store, and retrieve credentials for our databases and other services

Data Schema

A diagram showing how data flows through our systems (processing and storing) is shown below.



Sharing Data

As Sapia.ai is a global organization, our team need to share and access data worldwide. This enables us to provide you with software and user support. We have an intra-group data transfer agreement enabling the lawful transfer of this data (including outside the European Economic Area and the United Kingdom).

Like most organizations, we also use third-party services and tools to provide the Platform and Services. These are known as sub-processors.

Our sub-processors (who may process data outside the customer's sovereign location) are reviewed for security governance and controls. In addition, we enter into Data Processing Agreements with our third parties and suppliers, where we are required to do so by data privacy legislation.

As of July 2022, we only use Amazon Web Services (AWS) as a sub-processor.

Sub-processor	Storage Location	Function	Data Processed
AWS	In your region	Compute services Candidate communications Product analytics and user event tracking	-PII, including: Candidate name Candidate email address Candidate phone number -Demographic info (if known) -Browser information -Location from IP address -Open & link tracking -Candidate IP address -Interview Data -Customer Data

4 Data Protection

This section explains how Sapia.ai protects PII, Candidate and Customer Data.

Vendor Dependencies and Agreements
Sapia.ai has standard vendor agreements that include clauses related to privacy and security so that we ensure third party handling of our information is secure.

We manage the risks of handling information with third parties through our risk register and ensure we review their security and privacy positions annually.

End user identity and access control
The Sapia.ai platform offers a web app for hiring managers and recruiters to log in to check candidate results and receive insights on those candidates ("Edge"). The identity of the users is maintained inside the platform against the customer account. Users can be added and removed from the account.

The passwords defined against the login for the user have password complexity and age requirements. Access is also controlled via Multi-Factor Authentication (MFA) and/or Single Sign-On (SSO) to provide a further layer of security.

The actions a user can take on the system are governed by the roles, organizations, and/or departments assigned to them. Roles are used to restrict access to the functions of the system. In this way an identified user is only presented the functions and candidates they are authorized to access by the customer administrator.

System Administration Identity and Access Control
The Sapia.ai developers and operational staff that maintain the platform are identified by their AWS accounts.

The level of access to the Sapia.ai infrastructure is governed by the AWS Identity Access Management (IAM) system comprising security roles that grant the users access to the products and services. Each employee is given the minimum access to fulfill their role.

Audit, Alerting, Malware, and Incident Response
The actions of system administration users are monitored using AWS CloudTrail. CloudTrail allows all infrastructure actions to be reviewed, monitored, and alarmed.

The platform has many servers across AWS regions. The servers are like regular computers and run Windows or Linux operating systems. As such, they are vulnerable to the same malware as our own desktop systems. Sapia.ai has installed malware detection software into the servers to mitigate this vulnerability.

Sapia.ai has a security incident management policy that describes the procedure to be followed should an incident occur where we are concerned that security has been breached or compromised. This policy explains how we should notify stakeholders in accordance with data protection legislation.

Contingency Planning and Disaster Recovery
Sapia.ai is a SaaS-based business, and our computing infrastructure is based in the cloud. As a result, Sapia.ai have detailed plans for recovering from an incident or crisis. The method is tested annually to ensure all parties know how to respond and manage the incident.

We have a recovery time objective of 6 hours and a restore point objective of 24 hours. This means that in the event of the loss of an availability region in AWS, Sapia.ai can restore from the previous day's data and be up and running in 6 hours.

Configuration and Risk Management
When assessing data security and protecting it from misuse, Sapia.ai has a risk register that is reviewed annually and from which risk mitigations are planned. This means we consider how security may be breached and plan to mitigate the effects of a breach on a given data asset.

We also have a less formal means for any team member to raise any issues they think have arisen. We have set up a dedicated channel called 'security-and-privacy' within our communication tool "Slack". Again, this reflects the importance of the data asset we maintain.

One of the risks to the security of that data is the configuration of the systems that maintain it. Knowing how all the pieces fit together is vital for restoring services. Rather than this knowledge being only known by select staff, the ability is written in code so that any engineer with the proper authorization can recreate our environment.

Thus, our configuration vulnerability is mitigated by our investment in 'infrastructure in code' through Terraform. Further, we use a software deployment technology called BuildKite that can deploy new versions of software without human intervention. This mitigates any loss caused by outages by making recovery quick and systematic.

Data Center Security
AWS provides servers and infrastructure in several availability regions throughout the world.

They specialize in owning and operating some of the largest data centers in the world. Amazon's physical infrastructure has been accredited under ISO 27001, SOC 1/SOC 2/SSAE 16/ISAE 3402, PCI Level 1, FISMA Moderate, and Sarbanes-Oxley.

Network Security
Disciplined application infrastructure management is required to mitigate security risks while delivering excellent application performance and scalability.

Our infrastructure is managed using Terraform or 'infrastructure as code'. This modern practice improves the old way of setting up networks and servers, where network engineers must manually set up all the pieces required for an application. With Terraform, the infrastructure is described in code and executed at the press of a button. As a result, our infrastructure can be restored in hours rather than days. It also ensures we have fine grained control over the construction of our data center resources.

Sapia.ai uses the Virtual Private Cloud (VPC) technology from AWS to isolate services exposed to the public internet from those for internal processing. For example, the Chat Interview candidate experience (CX) is publicly exposed to the internet so browsers can access the service. However, the database and APIs for managing the prediction, organisation, and user data are hidden from the internet via a VPC.

Our APIs are managed behind AWS Gateway, meaning we can securely access, handle the load, and defend them successfully.

Activity is logged across the applications and networks so that in the event of an application, security, or privacy issue, we can investigate and trace the pieces impacted.

We run annual security audits and penetration tests to verify the effectiveness of the security controls we have in place.

Our servers are patched through a monthly review process, and user identity and authorities are reviewed within the same cadence.

Sapia.ai Employees
We use Jamf to control the MacBooks in use across the organisation. With this tool, we can audit compliance and automatically distribute software required (for example, virus scanning software).

All employees are required to complete annual training on data privacy and best practices for securing and handling user data.

All employees undergo thorough background checks executed by a Tier 1 vendor as a prerequisite for employment. In the UK, employees are vetted to Baseline Personnel Security Standard (BPSS) level.

Information systems acquisition, development, and maintenance
Sapia.ai operates an agile process for new and existing systems development. Source code control is maintained using GitHub with an approval process for code based on the GitHub 'pull request' technique.

Only staff with an operational need have access to PII, Candidate, or Customer data. This is also time limited to the period they require to perform the functional task.

We continually evaluate the security of our designs and test for security-related issues while we develop new products.

Security Documentation
Sapia.ai is accredited to ISO 27001 and SOC (Type 1). SOC Type 2 accreditation is ongoing. We have documentation that defines our security and privacy policies, and these are reviewed annually and published to the business and staff to check.

We manage risks, assets, and incidents in registers and a regular cadence of review and mitigations.

Change Management Maturity
Sapia.ai manages changes to the production environment technically using a continuous deployment system. The code covers infrastructure, configuration, and code; hence, change control is tightly executed across development, sandbox, and production environments.

Compliance
Sapia.ai has controls in place to meet GDPR and the Australian Privacy Principles. We have audits on our controls in line with our annual vulnerability assessments.

Breach Notifications
We treat breaches with the highest level of urgency. We are committed to delivering timely communications to customers who might be impacted. Any violations will be communicated within 72 hours. Of course, any data breach where we are the Data Controller will be reported to the relevant supervisory authority if it's a notifiable event. While acting as Data Processor, the Data Controller must notify the supervisory authority.

Important to note: There have been no recorded breaches to date.

5 Data Management & Destruction

Sapia.ai does not retain any personal data for any longer than is necessary for the purpose(s) for which that data is collected, held, and processed. Personally Identifiable Information (PII) and Customer Data is retained by Sapia.ai following your requirements as you remain the data controller.

Sapia.ai retains De-identified Derived Data indefinitely to build and maintain predictive models as well as create analytical and statistical data to improve or modify the services or develop new products.

Data Management
Different types of Personal Data, used for different purposes, will necessarily be retained for different periods, as set out on the following page.

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data can be regularly reviewed against those criteria.

Notwithstanding the following defined retention periods, specific Personal Data may be deleted or otherwise disposed of before the expiry of its defined retention period in response to a request from the data controller.

Data Destruction
Upon the expiry of the data retention periods set out on the following page, or when a request is received from the data controller, Personal Data shall be deleted, destroyed, or otherwise disposed of as follows:

- Personal Data stored electronically (including any and all backups thereof) shall be deleted
- Special category Personal Data stored electronically (including any and all backups thereof) shall be deleted

Data Type	Purpose	Retention Period	Comments
Candidate Personally Identifiable Information (PII)	Used to distinguish candidates and report recommendations (predictions)	In accordance with the customer retention period	At the point of deletion, Sapia.ai anonymises this data to become de-identified derived data
User Personally Identifiable Information (PII)	Used to provide hiring managers and recruiters access to the Sapia.ai platform	12 months following the conclusion of the contract between us unless the data subject requests deletion	
Demographic Data	Used for the purposes of reporting and bias testing of the AI at an aggregate level	In accordance with the customer retention period	At the point of deletion, Sapia.ai anonymises this data to become de-identified derived data
Interview Data - Chat Interview	Used for the hiring organisation to view candidate responses and for Ai analysis by Sapia.ai	In accordance with the customer retention period	At the point of deletion, Sapia.ai anonymises this data to become de-identified derived data
Interview Data - Video Interview	Used for the hiring organisation to view candidate responses	180 days or in accordance with the customer retention period	Data is completely deleted at the end of the retention period
ATS Assessment Requests	Used to request an assessment (or interview) for an applicant	7 years	Retained in the event of a legislative dispute
Metadata on the organisation and vacancies	Used to identify the hiring organisation, department structure and vacancies under hire	7 years or at the conclusion of the contract	Retained in the event of a legislative dispute
Behavioral Data	Pseudo anonymized data used to track and analyse user behavior across the system	Indefinite unless the data subject requests deletion	
De-identified Derived Data	Used for training and for R & D to discover more features for all customers	Indefinite	De-identified processed data that has been combined, aggregated or adapted to such a degree that it: (i) cannot be identified as originating or deriving directly from a specific individual and cannot be reverse engineered such that it can be so identified (ii) is not capable of use substantially as a substitute for the original data; and (iii) is not Personal Data.

Ownership and review

The CEO is the responsible owner of this document. This policy will be reviewed annually or earlier by CEO

Authorisation & approval

Barb Hyman - Sapia.ai CEO

Document History

12 Aug 2021	Jon Daye	V1.0	New Document (based upon *How we use and protect Data*)
17 Aug 2021	Jon Daye	V1.1	Addition of *Management & Destruction of Data*
28 Sep 2021	Jon Daye	V1.2	Removed references to NamSor
05 Oct 2021	Jon Daye	V1.3	Removed Postmark and Mixpanel, which are no longer used. Replaced with AWS Pinpoint & Kinesis
14 Jan 2022	Michael Zhang	V1.4	Added detailed graph on data sovereignty and data anonymization process.
20 Jul 2022	Jon Daye	V2.0	Rebranded as Sapia.ai and a general refresh


sapia.ai