Cloud Platform Technical Overview

Using SOPHiA DDM™ solution and cloud service

A cloud-native platform with information security at its core[1]

[1] For Research Use Only

DISCLAIMER

This document and its contents are the property of SOPHiA GENETICS SA and its affiliates ("SOPHiA GENETICS") and are intended solely for the contractual use by its customer in connection with the use of the service(s) described herein and for no other purpose. This document and its contents shall not be used or distributed for any other purpose and/or otherwise communicated, disclosed, or reproduced, or referenced to in any way whatsoever without the prior written consent of SOPHiA GENETICS.

SOPHiA GENETICS does not convey any license under its patent, trademark, copyright, or common-law rights nor similar rights of any third parties by this document. The instructions in this document must be strictly and explicitly followed by qualified and adequately trained personnel to ensure the proper and safe use of the service(s) described herein. All of the contents of this document must be fully read and understood before using such service(s).

SOPHiA GENETICS DOES NOT ASSUME ANY LIABILITY ARISING OUT OF THE IMPROPER USE OF THE SERVICE(S) DESCRIBED HEREIN (INCLUDING PARTS THEREOF OR SOFTWARE).

REVISION HISTORY AND APPROBATION

Document version	Date	Status
1.0	January 29th 2025	Initial release

PERIOD OF VALIDITY

The document of valid for a maximum of 24 months.

Required changes may be introduced at any time, particularly if required by law.

Table of Contents

1 Who we are

1.1 Our mission

SOPHiA GENETICS was founded to generate clinically actionable insights from data to improve patient outcomes. Our mission is to provide equal access to knowledge and capabilities by democratizing data-driven medicine.

We observed that across the healthcare ecosystem, a vast amount of digital healthcare data was being generated, fueled by technologies such as NGS, and which held promise to accelerate the understanding of biology and disease. However, this data has been generated primarily using non-standardized methods and by clinicians and researchers across many healthcare institutions. As a result, the data remained siloed and complex and was not fully leveraged for the benefit of patients.

We founded SOPHiA GENETICS to address this issue. We are unlocking data silos, leveraging AI to generate actionable insights from data and helping healthcare professionals work together as a community and deploy their collective expertise for the benefit of patients around the world.

We are a cloud-native software technology company in the healthcare space dedicated to establishing the practice of data-driven medicine as the standard of care and for life sciences research. We purposefully built SOPHiA DDM™ a cloud-native software platform capable of analyzing data and generating insights from complex multimodal data sets and different diagnostic modalities. Our platform standardizes, computes and analyzes digital health data and is used across decentralized locations to break down data silos.

We believe that a decentralized platform is the most powerful and effective solution for creating the largest network, leveraging data, and bringing the benefits of data-driven medicine to customers and patients globally. In doing so, we can both support and benefit from growth across the healthcare ecosystem.

For more information on SOPHiA GENETICS its product, and its strategy, please visit www.sophiagenetics.com

1.2 Our headquarters and offices

SOPHiA GENETICS has offices in the following locations:

Headquarter

SOPHiA GENETICS SA
ZA La Pièce 12
1180 Rolle
Switzerland

Subsidiaries

SOPHiA GENETICS Inc.
185, Dartmouth Street, Suite 502
Boston, MA 02116
USA

SOPHiA GENETICS S.A.S
Technopole Izarbel
158 allée Fauste d'Elhuyar 64210 Bidart,
France

SOPHiA GENETICS S.R.L
Via Michelangelo Buonarroti 39, 20145, Milano

SOPHiA GENETICS LTDA
Av. Lauro de Gusmão Silveira, No. 479, sala 01,
Jardim São Geraldo, CEP: 07140-010,
Guarulhos, SP

SOPHiA GENETICS Limited
60 Windsor Avenue, London,
United Kingdom, SW19 2RR

SOPHiA GENETICS PTY LTD
QLD 4000, Australia

1.3 Governing laws and authorities

For customers based in France, Italy, Brazil, the United States, Canada, the United Kingdom, and Australia, the usage of the SOPHiA DDM™ Platform and contractual agreements are governed by the respective local laws of each country.

For customers in any other country, the governing law is Swiss law.

Regarding data protection, compliance is determined by the legal requirements of the country where the data is processed and/or the country of origin of the individual whom data are processed, depending on local regulations.

Since SOPHiA GENETICS processes data in various server locations[2], the following regulations and standards apply based on the region:

- Europe: GDPR (General Data Protection Regulation)
- Brazil: LGPD (Lei Geral de Proteção de Dados)
- United States: HIPAA (Health Insurance Portability and Accountability Act)
- Switzerland: FADP (Federal Act on Data Protection)
- Canada: PIPEDA (Personal Information Protection and Electronic Documents Act)
- Australia: Privacy Act 1988
- UAE: DPL (Data Protection Law) DHCA (Dubai Healthcare City Authority)
- Turkey: KVKK (Law on the Protection of Personal Data).

[2] See Section 6 Servers physical and service localization

1.4 How to contact us

We're here to assist you with any inquiries you may have. To help us direct your request to the right team, please select the appropriate contact based on your needs:

Data Protection Officer (DPO)
You have concerns about how we handle personal data. You have questions related to our privacy policies or requests regarding data access, deletion, or updates. You want to report any data privacy incidents or violations.

- Email: privacy@sophiagenetics.com

Customer Service

You need help with orders, product inquiries, or account issues. You have questions around SOPHiA DDM account usage or product shipping. For any general inquiries regarding your account or service experiences.

- Email: support@sophiagenetics.com

Security Issues

You need to report security vulnerabilities or concerns related to our systems, websites, or services. For incidents such as suspicious activities, phishing attempts, or account security breaches.

- Email: Security@sophiagenetics.com

General Information

For all general inquiries not covered by the specific categories above. For information about our company, policies, partnerships, or media requests.

- Visit: https://www.sophiagenetics.com/company/contact/

2 Overview of SOPHiA DDM™ platform

2.1 Introduction to our Cloud-Native solution

The SOPHiA DDM™ platform is a powerful cloud-native solution designed for analyzing complex genomic and multimodal health data. Hosted on Microsoft Azure, it leverages Azure's robust cloud infrastructure to provide secure, scalable, and compliant data processing capabilities, essential for advancing precision medicine.

By utilizing Azure, SOPHiA DDM™ benefits from the cloud's high availability and global reach, enabling healthcare providers, research institutions, and biopharma companies to analyze vast amounts of health data efficiently.

The Azure instances are all owned by SOPHiA GENETICS and managed by the cloud service provider (Microsoft) to deliver the best services to customers.

When using the SOPHiA DDM™ platform, SOPHiA GENETICS' customer's data are stored and processed in a cloud environment secured using the highest industry standards, allowing users to analyze their data securely. Customers can apply additional security measures intended to protect further patients' data and privacy. The following document is intended to provide the cloud service customer with all information required in accordance with ISO 27001: 2022, ISO 27017:2015 and ISO 27018:2019 requirements.

2.2 Certifications

SOPHiA GENETICS holds the following certifications:

- ISO 27001:2022 Information Security Management Systems
- ISO 27017:2015 Security Techniques - Cloud Service Provider and Cloud Service Customer
- ISO 27018:2019 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO 13485 – Quality Management System

2.3 Intellectual property and licenses

As between Customer and SOPHiA GENETICS, all right, title, and interest in and to the SOPHiA GENETICS Technology, including all intellectual property rights, remains the sole and exclusive property of SOPHiA GENETICS.

SOPHiA GENETICS grants customers simple user licenses limited to the duration of the contract.

2.4 Data Ownership

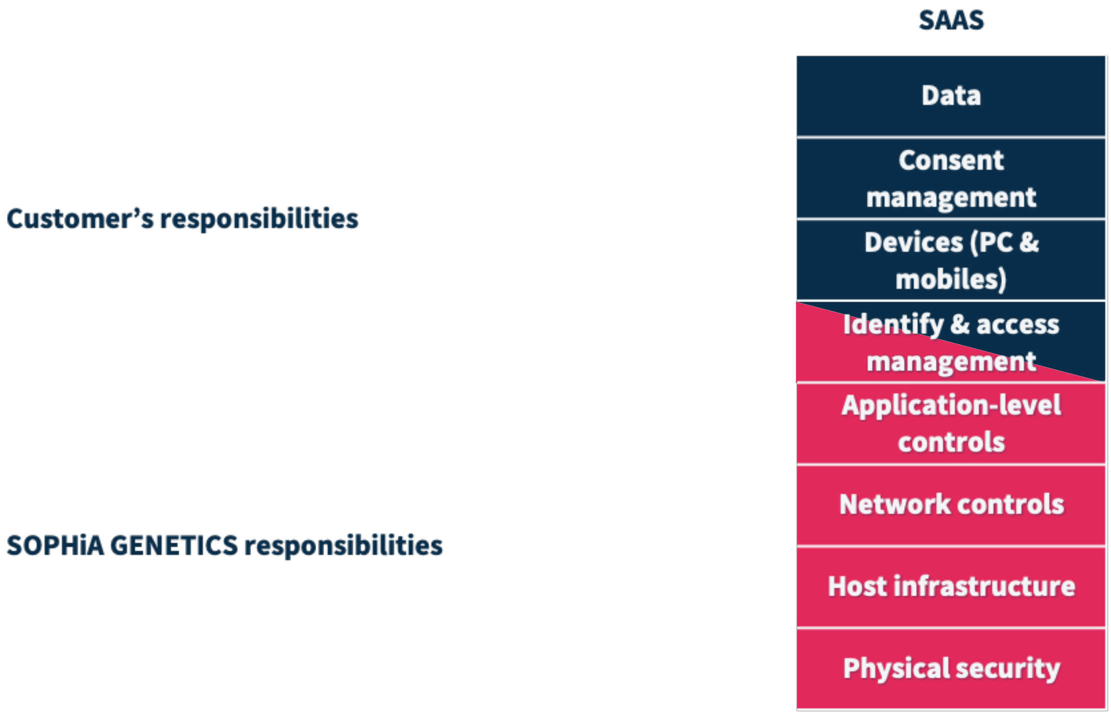
Our customers retain full ownership of all their data when using our SOPHiA GENETICS Technology or Products. Customers are responsible for ensuring that the data used and included into SOPHiA GENETICS Technologies are legal, reliable, and accurate. While maintaining ownership, the customer grants SOPHiA GENETICS permission to access and use data for specific purposes, such as performing our services, conducting research, and improving our products.

3 Roles and Responsibilities in the provision and maintenance of cloud services

SOPHiA GENETICS has partnered with Microsoft Azure to provide its SOPHiA DDM™ Platform, leveraging Azure's robust computing capabilities to offer customers cutting-edge solutions. By adopting a Software as a Service (SaaS) model, SOPHiA GENETICS enables its clients to benefit from the scalability, reliability, and advanced infrastructure of the cloud, reducing the need for significant on-premises hardware investments.

In traditional on-premises datacenters, customers are fully responsible for all technical tasks, including the administration, configuration, and maintenance of their information systems. However, in a SaaS model, a portion of these responsibilities shifts to the service provider, allowing customers to focus patient care and research while relying on the provider for system management and security.

The following figure outlines the division of responsibilities between the customer and SOPHiA GENETICS when using the SOPHiA DDM™ Platform.


SAAS
Customer's responsibilities
SOPHiA GENETICS responsibilities
Data
Consent management
Devices (PC & mobiles)
Identify & access management
Application-level controls
Network controls
Host infrastructure
Physical security

Please find below – shared responsibility in the cloud: [Shared responsibility in the cloud - Microsoft Azure | Microsoft Learn]

As a solution fully hosted in the Microsoft Azure cloud, Data Center physical security falls under Microsoft Azure's aegis. Microsoft Azure's security certifications are available in the [Microsoft Service Trust Portal].

4 Data processing in the cloud

The cloud-native platform SOPHiA DDM™ is designed to analyze complex genomic and healthcare data, leveraging cloud infrastructure. The platform standardizes multimodal datasets, such as genomic and clinical information, to generate insights that can aid healthcare professionals in diagnosing diseases, particularly cancer and rare diseases.

The following sections present how the data are processed, stored, and secured in the SOPHiA DDM™ Platform.

4.1 Definitions

The data are defined as follows:

- **Personal data:** any information allowing to identify directly or indirectly an individual;
- **Personal Identifiable Information (PII):** A term commonly used in the United States to refer to specific types of personal data that can be used to identify an individual.
- **Sensitive personal data:** These include genetic data, ethnicity, or health-related information.
- **Protected Health Information (PHI):** It refers to any health information that can be linked to an individual and is protected under regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States
- **Direct identifying data:** data points that can be used to identify a person solely based on the data available (first and last name). This is also data that is unique to a person (e.g. social security number);
- **Indirect identifying data:** Data points that do not immediately identify a person on their own but could be used in combination with other information or sources to re-identify an individual.
- **Non-personal data:** this is data that is not linked to a person and cannot be used to identify someone directly or indirectly;

4.2 List of data processed

Categories of data	Retention	Recipients
Patient or Individual[3]		
Direct identifying data:		
Identity: name, surname of the individual	As per the contract agreement (commonly 5 years). An additional retention of 10 years could apply on specific products to satisfy legal obligations or/and preserve the company's right to defense.	User's partners or colleagues through the extracted report - Data Processor and its sub-processors
Contact details: address, email address and phone numbers.		
Other data that could be recorded by the user in the *Conclusion* section of SOPHiA DDM™[4]		
Indirect identifying data (quasi-identifiers):		
Identifier: Identifier allocated to the patient by the Customer	As per the contract agreement (commonly 5 years). An additional retention of 10 years could apply on specific products to satisfy legal obligations or/and preserve the company's right to defense.	User's partners or colleagues through the extracted report - Data Processor and its sub-processors (see dedicated section)
Identifiers: SOPHiA GENETICS identifier allocated to the individual or patient, Institution identifier allocated to the customer		
Gender		
Ethnicity and origin		
City of residence		
Date of birth		
Genomic data and related metadata (date, location, quality of biological sample analysis)		
Health data including disease, anamnesis, comments from the platform user about the individual or patient (e.g., health-related habits).		
Users		
Direct identifying data:		
Identity: name, surname, professional email address, phone number	As per the contract agreement (commonly 5 years). An additional retention of 10 years could apply on specific products to satisfy legal obligations or/and preserve the company's right to defense.	Data Processor and its sub-processors
Indirect identifying data (quasi-identifiers):		
Log-in details and password	As per the contract agreement (commonly 5 years). An additional retention of 10 years could apply on specific products to satisfy legal obligations or/and preserve the company's right to defense.	Data Processor and its sub-processors
Activity on the platform and logs		
User's employer		

[3] *The individual family members' data may be collected in the context of specific products available on SOPHiA DDM*

4 The customer undertakes not to include any personal data in the free text fields at the end of the study report in order to preserve the pseudonymization of the data.

4.3 SOPHiA GENETICS list of sub-contractors

Name: Microsoft Ireland Operations Limited, c/o Microsoft Schweiz GMBH

Address: Richtistrasse 3, CH-8304 Wallisellen, Switzerland

Description of processing: Cloud services

Name: Databricks Inc.

Address: 160 Spear Street, Suite 1300, San Francisco, CA 94105, USA

Description of processing: Data governance & security

Name: Endava GmbH

Address: Eschersheimer Landstraße 14, 60322 Frankfurt am Main, Germany

Description of processing: data visualization (engineering support)

Name: Atlassian

Address: Singel 236 1016 AB, Amsterdam, Netherlands

Description of Processing: Customer support, processing users' data only.

Do you want to know more?

SOPHiA GENETICS offers its customers detailed compliance documentation regarding processing personal data on the SOPHiA DDM™ platform. This includes comprehensive reports such as Data Protection Impact Assessments (DPIA), which outline how data is processed, identify potential risks, and define both our responsibilities and those of our customers. Additionally, we provide Data Processing Agreements (DPA) and other key compliance materials to ensure full transparency and legal protection.

5 Technical architecture

5.1 General SOPHiA DDM™ architecture

SOPHiA GENETICS provides a SaaS solution for its customers allowing to upload genomic data onto the platform, conduct the analysis and issue a report. Data is hosted on SOPHiA GENETICS' infrastructure, based on Microsoft Azure technologies. Customers can access SOPHiA GENETICS services via a locally installed agent on the customer's site.

The services are accessible from a local application and soon from a full web portal of New generation of SOPHiA DDM™.

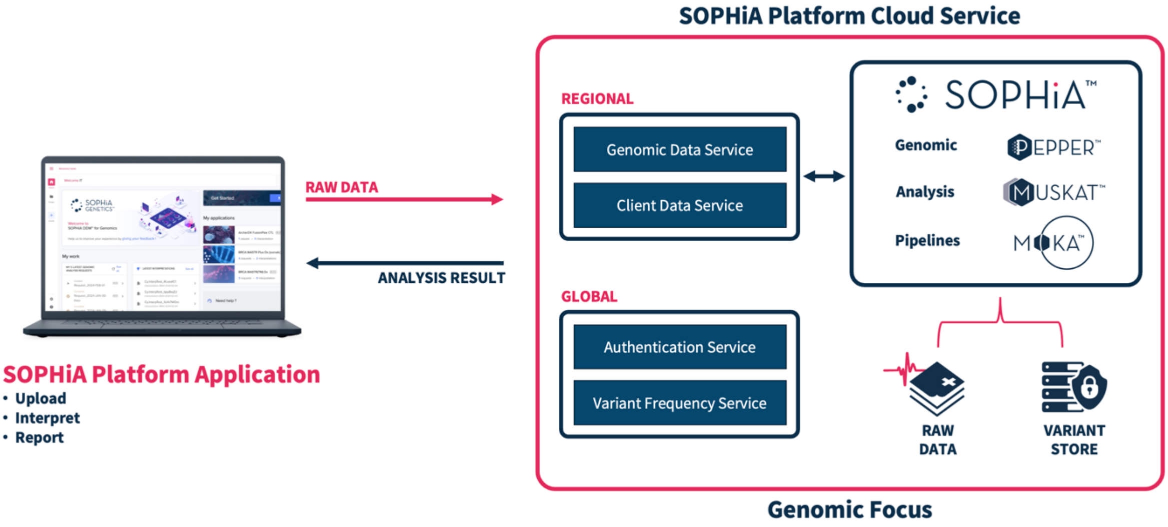


Fig 1: SOPHiA DDM™ High level overview[5]

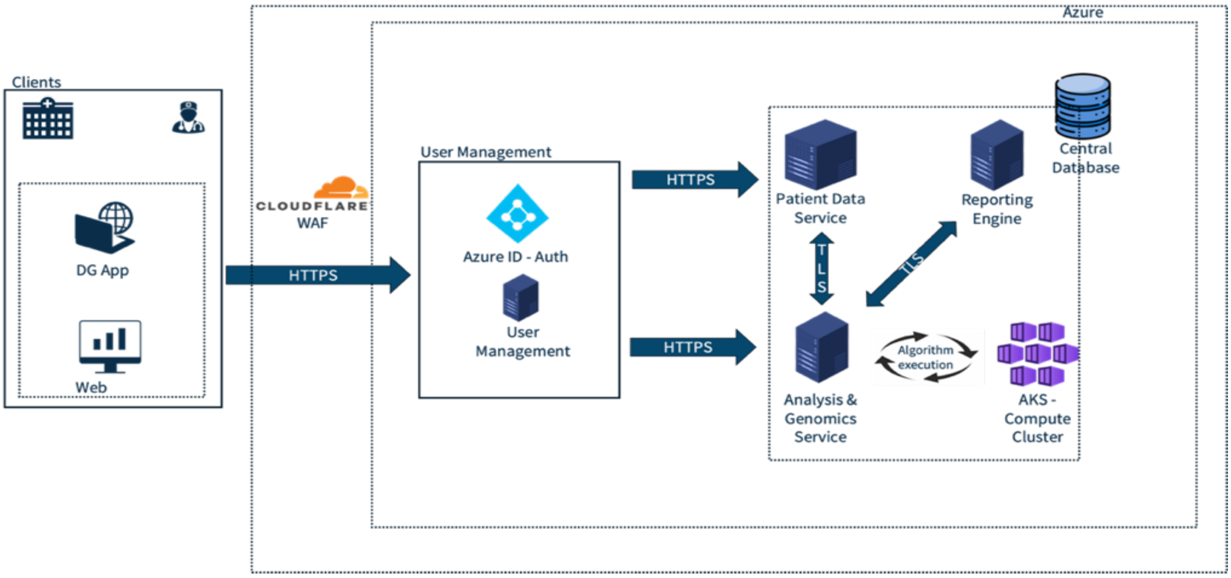


Fig 2: SOPHiA DDM™ Component by region

Further information can be found in the product technical documentation available online.

[5] The figure below provides an overview of the architecture. For confidentiality reasons, the figure provided remains high-level, and the customer is welcome to request further details.

6 Servers physical and services localization

SOPHiA DDM™ is fully hosted in the Microsoft Azure cloud, leveraging a hub-and-spoke architecture. The SOPHiA Platform is distributed to a “decentralized” customer base - enabling patient data and patient-centric reporting to stay local - data uploaded to the SOPHiA Platform by the Customer is transferred and integrated into a “centralized” series of regional data warehouses used by SOPHiA GENETICS. Customer data and compute resources powering our analysis capabilities are hosted in specific cloud regions to comply with local legal and regulatory requirements.

Core services, such as billing and invoicing management, are hosted in a central hub.

Azure resources used for and by SOPHiA DDM™ are located in the following locations and regions.

Customers Location	Type of service	Server Location	Azure Region
All region	Cores Services[6]	Europe	West Europe
Europe	Customer data & compute resources	Europe	West Europe (Netherlands) Hébergeur de données de Santé certified
France	Customer data & compute resources	France	France Central Hébergeur de données de Santé certified
Switzerland	Customer data & compute resources	Switzerland	Switzerland North
United States	Customer data & compute resources	United States	US East 2
Brazil	Customer data & compute resources	Brazil	Brazil South
Canada	Customer data & compute resources	Canada	Canada Central
Australia	Customer data & compute resources	Australia	Australia East
United Arabs Emirates	Customer data & compute resources	United Arabs Emirates	United Arabs Emirates

Customer data are located in the customer's region in accordance with applicable cross-border data transfer laws and regulations[7].

By default, Azure virtual machines and services operate on UTC (Coordinated Universal Time) and synchronize their clocks using the Microsoft time synchronization service. This service ensures accurate timekeeping across all Azure resources by leveraging NTP (Network Time Protocol) for consistent time synchronization with reliable time sources.

6.1 Volume Capacity

SOPHiA DDM™ platform and related cloud infrastructure offering is designed to provide scalability and meet our customers’ needs effectively with:

- **Multitenant infrastructure:** the platform operates on a multitenant infrastructure to efficiently handle multiple users or customers simultaneously within a single, shared

[6] Billing and invoicing management

[7] Customer data can be located in a different region upon customer notification and approval

environment. This setup allows for high flexibility and resource optimization, ensuring that customers have the capacity they need without having to manage physical hardware.

- **Horizontal scalability:** Our infrastructure is designed to scale horizontally. This means that if customer demands increase or if additional processing power is required, SOPHiA GENETICS can easily instantiate more instances or nodes to accommodate customers' needs. This scalability ensures that you can handle larger loads and maintain performance even as your requirements grow.

- **Processing capacity:** In terms of processing capacity, we can handle a substantial volume of samples analysis at the same time to ensure customers can conduct their analysis simultaneously.

- **Flexibility and performance:** With our offering, you benefit from the flexibility to scale up as needed and the assurance of consistent performance. Whether you're experiencing a temporary surge in data or have a steady flow of samples, our infrastructure adapts to ensure your operations run smoothly.

The volume of platform and cloud resources allocated to a customer is directly linked to the number of analyses purchased for the specific product. The customer's access to storage, processing, and usage capacity is limited to the volume required to perform the analyses they have acquired. The platform is designed to comfortably accommodate the normal volume of analyses typically conducted by a laboratory. However, any additional analyses or increased usage beyond the allocated volume will require the purchase of additional capacity to ensure continued access and performance of the platform.

6.1.1 Monitoring and tracking

SOPHiA GENETICS monitors its cloud service activities using visualization, monitoring and alerting. Through dynamic dashboards providing real-time insights into system performance, application health, business metrics, preventing downtime and maintain the SOPHiA DDM™ services available to customers.

SOPHiA GENETIGS monitors its cloud service operation using the following monitoring tools and services:

Infrastructure monitoring:

- Server health monitoring: CPU, memory, disk usage, and network I/O.
- Kubernetes and container monitoring: Track the status of pods, nodes, and services.
- Cloud resource monitoring: Track metrics from Azure cloud platforms

Application Performance Monitoring (APM):

- Monitor application performance, response times, and error rates using metrics from APM tools or custom instrumentation.
- Visualize request latencies, HTTP status codes, and database query performance.

Security Monitoring:

- Monitor security-related events and anomalies
- Alerting system: If a metric exceeds or drops below a certain threshold, Architecture and Cybersecurity Team is notified and could decide to open incident management process.

7 Account and access management

7.1 Customer account management

SOPHiA GENETICS offers a robust platform featuring advanced access management, which allows customers to manage user rights effectively. This granular control ensures that sensitive information is protected while enabling user collaboration.

7.1.1 User account creation

Each Institution provides a list of individual system users and email addresses used as usernames. Each user will also receive an initial password and a token card. The password shall be updated upon first login onto the system. To log in, the user must enter his/her username and password and will be prompted for a specific security code to be read from the token card. Upon 5 failed attempts, the user login will be blocked, and the administrator must request SOPHiA GENETICS to re-activate the login. If the password is forgotten or the token card is lost, customers are advised to contact SOPHiA GENETICS Customer Support.

The following strong authentication methods are supported:

mTAN	The mTAN login combines the entry of a username and password with that of a code sent to the cell phone.
Code Card	By default, the user created has a registered code card for his or her username. Entering a password and a username is combined with the registration of one of the codes present on the card at a given position at the time of entry.

The authentication layer is very flexible and supports several different authentication methods. Microsoft's Azure products are used to meet the needs (access control, management of identity avec MFA).

7.1.2 User account management

Various user groups are established within the system, each with distinct permissions tailored to their specific roles. For detailed information about the different user groups and their respective rights, please refer to the "Operational Manual."

Each institution is responsible for managing its users and maintaining user access up to date. The institution is also responsible for identity checks, changes to rights, and account deletions and for providing SOPHiA GENETICS with an up-to-date list of people and rights to apply.

All users receive a confirmation email at account creation, change of rights, or deletion. From time to time, SOPHiA GENETICS sends notifications to users about security information, new platform release features, or updates.

For more information regarding registration and authentication to the platform visit: https://www.sophiagenetics.com/document/sophia-ddm-core-platform-user-manual/

In the event that Platform credentials are compromised, the customer must promptly contact Customer Service to enable the Company to secure the account and block any unauthorized access that may jeopardize the customer’s account.

Email: support@sophiagenetics.com

7.2 SOPHiA GENETICS internal cloud account management

SOPHiA GENETICS adheres to a strict policy of using nominative accounts exclusively for the management of its cloud services. These accounts are assigned to individual users, ensuring accountability and traceability. Shared or service accounts are not used, aligning with best practices for enhanced security and operational transparency.

7.2.1 Defined Roles for Cloud Management

SOPHiA GENETICS maintains the following clearly defined roles to manage and secure its cloud services effectively:

1. Administrative Accounts

- **Global Administrator**: Full access to all Microsoft Entra ID and Azure services.
- **Privileged Role Administrator**: Oversees role assignments and manages privileged identity management.
- **User Administrator**: Handles user and group management, including password resets.

2. Security-Focused Accounts

- **Security Administrator**: Configures security settings and accesses security-related data.
- **Security Operator**: Creates and manages security events.
- **Security Reader**: Reads security information and generates reports.

3. Application Management Accounts

- **Application Administrator**: Manages app registrations and enterprise applications.
- **Application Developer**: Independently creates and manages application registrations.

4. Read-Only Accounts

- **Global Reader**: Reads all accessible information but cannot make changes.
- **Report Reader**: Views sign-in and audit reports.

5. Basic Access Accounts

- **Directory Reader**: Reads basic directory information, typically for applications and guests.
- **Authentication Administrator**: Manages and resets user authentication methods.

7.2.2 Review and Compliance

All accounts provisioned within Microsoft Azure undergo at least an **annual review** to verify compliance with organizational security standards and operational requirements. This review ensures that access levels are appropriate and that inactive or unnecessary accounts are decommissioned.

8 Technical and organizational security measures

8.1 Technical security measures

SOPHiA GENETICS has implemented a robust security framework by designing its Technologies and its cloud infrastructure with compliance to regulatory requirements as a top priority.

Policies and procedures are deployed internally to ensure our customers' data remain secure at all times. A list of our internal policies and procedures are provided in the annex I.

The SOPHiA GENETICS architecture ensures security by design, integrating information security considerations into every phase of the software development lifecycle. By embedding security measures throughout the development process, we safeguard sensitive data and maintain the integrity of our platform, demonstrating our commitment to the highest standards of security and compliance.

8.1.1 Pseudonymization

The SOPHiA DDM™ platform uses a specific pseudonymization technique that segregates individual or patient data from direct identifying data. All individuals or patients' data and FASTQ or BAM files generated via sequencing technologies are linked to a randomized unique identifier generated by the platform. The direct identifying data, along with the corresponding randomized identifier, are stored in a separate server accessible only to a restricted number of SOPHiA GENETICS employees and according to strict access management procedures.

8.1.2 Encryption

All files are encrypted on the client computer during upload and remain encrypted in storage.

Encryption-in-transit is implemented for all customer data and according to the following rules:

- Channel encryption and server authentication must be achieved with TLS 1.2 or above.
- The channel-level encryption algorithm should be AES 256-bit or above.

Encryption-at-rest is implemented for all customer data and according to the following rules:

- Applies on all internal end-user devices (computers, phones, etc.), records, databases, disks, storage mediums, etc. using AES 256-bit or above.

8.1.3 Logical access control

SOPHiA DDM™:
The SOPHiA DDM™ platform's access model adheres to security controls applied by the SOPHiA GENETICS and includes, but is not limited to, internal Single Sign On access and provisioning, governed by the logical control mechanisms, including annual reviews of internal user accounts. The platform security is also assessed through penetration tests and vulnerability assessments to ensure that the account provisioning isn't exploited and is in accordance with the least privilege access model.

Microsoft Azure:
User profiles on Microsoft Azure are assigned based on their role in the company and applied via Active Directory groups. Any request for additional access rights is managed and approved on a dedicated ticket. Two-factor authentication (One-Time Code) is required to access internal

networks, applications, and data. Passwords must be at least 8 characters long and contain 3 of the following four categories: Upper Case, Special Characters, Numbers, and Lower Case. The Microsoft ATP module detects suspicious authentication attempts and alerts security.
If suspicious authentication attempts are made, a delay between attempts is activated to block denial of service.

8.1.4 Activities and log monitoring

All user activities, including function use, data addition, deletion, modification, and activity history, are monitored.

SOPHiA GENETICS continuously monitors the logs of its cloud platform services to maintain robust security. This enables the identification of potential threats and malicious activities while ensuring comprehensive oversight and rapid response to any anomalies. Through the tools, SOPHiA GENETICS can monitor users' logs and activities to identify and prevent suspicious behavior.
Access and activity logs are collected and retained to ensure cloud service security. All logs are analyzed and available for 90 days in the Security Center for analysis should an incident be detected.
Access granted to SOPHiA GENETICS systems generates logs that may contain personal data (PII). As for all personal data, SOPHiA GENETICS preserves individual rights that may be identified via the logs. Logs can only be used for activity tracking, auditing, and troubleshooting activities defined strictly in the privacy policy available in SOPHiA DDM™ Platform.

8.1.5 Web Application Firewall (WAF)

SOPHiA GENETICS uses Web Application Firewall (WAF) to protect its applications from malicious traffic. The firewall analyzes incoming requests and blocking access attempts that appear suspicious or harmful. The WAF is used by SOPHiA GENETICS to detect abnormal patterns, suspicious payloads, DDOS attacks, or access attempts from malicious IPs.
When a request is made to a protected website, the WAF evaluates it based on these rules. If it detects an attempt to exploit vulnerabilities, the WAF blocks or challenges the request, preventing unauthorized access or potential damage. It also provides insights into attack patterns and logs access attempts, enabling admins to monitor, fine-tune rules, and improve overall security.

8.1.6 Information classification and Data Loss Prevention

SOPHiA GENETICS uses a dedicated solution for Data Loss Prevention (DLP) and data classification, helping the company to protect sensitive information and ensure compliance with regulatory standards. SOPHiA GENETICS is implementing features to label and categorize data based on predefined policies, making it easier to manage and safeguard critical information while ensuring adherence to security and privacy requirements

8.1.7 Technical vulnerabilities management

In line with its longstanding commitment to information security, SOPHiA GENETICS has implemented a thorough vulnerability management process that is aligned with industry best practices and codified in a vulnerability management policy.
SOPHiA GENETICS uses an infrastructure vulnerability management tool, offering continuous visibility into the security posture of cloud environments. Scanning of the infrastructure allows to detect vulnerabilities such as outdated software, misconfigurations, missing patches, and other security gaps.

SOPHiA GENETICS uses various tools to identify and fix vulnerabilities in code, dependencies, containers, and infrastructure. Vulnerability scanning is integrated directly into development workflows to provide real-time vulnerability detection. Code repositories and the assets powering the SOPHiA DDM™ platform are scanned every week to identify vulnerabilities.

SOPHiA GENETICS prioritizes vulnerabilities based on risk, providing actionable insights by evaluating factors like exploitability, threat intelligence, and the criticality of the affected assets. It integrates seamlessly with other security tools, allowing for automated remediation workflows, reporting, and monitoring. This helps organizations proactively reduce their attack surface by identifying and mitigating infrastructure vulnerabilities before they can be exploited by attackers.

8.1.8 Penetration testing

To further fortify the security of our applications, we engage in comprehensive yearly penetration testing conducted by certified security professionals, ensuring the continuous identification and mitigation of potential vulnerabilities.

8.1.9 Security incident management

SOPHiA GENETICS maintains its product and services hosted on the Microsoft Azure cloud by ensuring the organization's information, as well as its reputation, are protected by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

This section outlines the collaborative Security Incident Management process between SOPHiA GENETICS and its customers applicable to all security incidents impacting the confidentiality, integrity, and availability of information or services managed within the cloud infrastructure.

Security Incident definition

A security incident is defined as any event that compromises or poses a risk to the security of systems, networks, or data, including but not limited to:

- Unauthorized access to data or systems.
- Data breaches or leaks.
- Denial of Service (DoS) attacks.
- Malware infections.

Responsibilities

SOPHiA GENETICS	Customers
• **Detection and Notification:** monitoring cloud environments and promptly detecting security incidents. • **Incident Analysis:** conduct a preliminary analysis to assess the impact of the incident, determine the affected assets. • **Incident Response:** initiate appropriate incident response measures, including containment, eradication, and recovery. • **Post-Incident Review:** review and defined the lessons learned and recommended corrective actions.	• **Notification:** The customer must notify SOPHiA GENETICS immediately if they detect any security incident affecting the cloud services. • **Cooperation:** The customer will cooperate with the provider's incident response efforts, providing any necessary information or assistance as required to mitigate the impact of the incident. • **Data Protection:** The customer is responsible for ensuring that any data they input and manage within the platform adhere to their internal policies.

• **Notify the customer:** notify the customer of major security incidents.	

Incident notification

The customer must notify SOPHiA GENETICS immediately if they detect any security incident affecting the cloud services by:

- Via mail (Security@sophiagenetics.com), or
- Via telephone +41(0) 21 694 10 60

SOPHiA GENETICS will inform the customer of a major information security incidents significantly affecting the availability confidentiality or integrity of data without undue delay. Should the incident have an impact on personal data, the customer will be informed within 48 hours to allow them to notify a potential data breach to the authorities.
The notification will contain the nature of the incident, affected services, initial impact assessment, and steps being taken for containment. Status updates will be provided to the customer until the incident is closed.

8.1.10 Backups management

Backup Plans

Backups of SOPHiA DDM™ platform data follow a specific and designated backup plan defined to ensure the Confidentiality, Integrity and Availability of customer data:

- **Backup methodology and frequency**

All backups are conducted on the secondary system, which is a replica of the master system, ensuring minimal disruption to production environments.
SOPHiA GENETICS conducts at least one full physical backup and one logical backup daily. For some specific databases considered key for the operations of SOPHiA DDM™, more frequent backups are conducted. These backups are scheduled at a defined time every day and allow a database-level recovery as well as a whole system recovery.
All backups are stored in the following formats:

- SQL format for database backups (e.g., .sql files).
- TAR format for file system backups (e.g., .tar archive files).

- **Backup location**

All backups are stored in the same region of the initial database to ensure compliance with data residency requirements. For more information regarding the location of servers, please refer to section §6.
To ensure availability and preservation of the data, it is replicated synchronously three times within a single physical location in the primary region. It is then copied asynchronously to a single physical location in a secondary region that is hundreds of kilometers away from the primary region.

- **Backup encryption and security**

The data is encrypted and an MD5 check is implemented during the analysis. All backups are secured in a dedicated blob storage with strict access management procedure and limited to identified individuals.

Backup integrity and testing

To ensure the reliability of backups, System Owners implement the following:

Backup Testing:

- Build scripts to perform full backups and upload them to the designated storage location.
- Simulate error conditions (e.g., incorrect commands or parameters) and display the appropriate error or status codes.

Backup Integrity Verification: System Owners must verify that backups remain unaltered after creation by using the following methods:

- **Hash generation**: A hash is created immediately after backup completion. This serves as reference point to confirm backup integrity over time.
- **Checksum creation**: A checksum is generated for comparison during restoration to ensure the backup has not been modified or corrupted.

8.1.11 Business Continuity and Disaster Recovery

In line with SOPHiA GENETICS Business Continuity and Disaster Recovery policy, and taking business need and contractual agreements, System Owners define processes to monitor and report on backup activities, including success, failure, and any errors. Specific guidelines include:

- **Restoration procedures**: Steps for manually restoring data from Azure Blob Storage or local backups (if available).
- **Recovery metrics**: Establish and track metrics for retrieving both physical and logical backups.
- **Recovery Objectives**: Clearly define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
- **Testing**: Schedule and document regular testing of backup and recovery procedures to ensure they meet business continuity standards.

8.1.12 Back-up Retention and Deletion

Backup plans are aligned with SOPHiA GENETICS Records Retention and Disposal policy and comply with applicable legal and regulatory standards. Backups of production databases containing patients' data are retained for a minimum of 6 years. This retention period is defined based on regulatory requirements (e.g. Health Insurance Portability and Accountability Act) and standard contractual agreements with customers.

8.2 Organizational security and privacy measures

8.2.1 Data protection: management rules

SOPHiA GENETICS has officially designated a Data Protection Officer (DPO) to the authorities and a Chief Information Security Officer. Information Security & Privacy Committees are held regularly and involve Data Protection, Cybersecurity, Information Security Governance and Legal departments.

8.2.2 Managing privacy risks

SOPHiA GENETICS conducts an annual enterprise risks identification, assessment and prioritization exercise aiming at defining risk mitigation action plan followed and implemented by risk owners. All project management follow the strict rules of design and change controls procedures with systematic processes used to ensure that the design of a product, system, or process, as well as any changes to it, are properly managed, documented, and controlled. It includes definition of specifications, Privacy Impact Assessment, Security Assessments and identification of remediation actions.

8.2.3 Managing personal data violations

Incident management is developed in a dedicated policy. All incidents are qualified, evaluated, and tracked. They are reviewed every month by the Information Security and Privacy committee. Where an incident result in a breach of personal data, the dedicated data breach policy is activated for responding to and managing data breaches in order to minimize their impact on an organization and the individuals affected. This policy outlines the steps to identify, report, investigate, and resolve breaches involving sensitive information, ensuring that the organization complies with legal, contractual and regulatory requirements while protecting data integrity.

8.2.4 Personnel management

All employee contracts include a clause on cybersecurity responsibilities:

- Employees are subject to secrecy and confidentiality after their contract termination;
- Employees receive specific training/awareness in cybersecurity with a focus on the cloud
- Employees are informed of their legal liability in the event of a breach of data security aspects;
- Employees are informed of their responsibility in the event of non-compliance with the security rules set by the company
- Employees are informed of their responsibility for data processing.

SOPHiA GENETICS oversees the training of its employees regarding the appropriate use of personal data. Users are also required to maintain the confidentiality of individual or patient data.

All SOPHiA GENETICS new employees need to accept the Acceptable Use of Information System policy and undergo awareness training on security issues (passwords, information management, phishing, social engineering, etc.) and personal data protection. When leaving the company, SOPHiA GENETICS employees, as well as subcontractors, have their access withdrawn by deactivating their active directory accounts and the related accounts tracked in their HR ticket.

8.2.5 Physical access control

Access to the premises and server facilities is restricted via badges, and only authorized persons have access.

8.2.6 Access for internal SOPHiA GENETICS employees

SOPHIA GENETICS applies the principle of least privilege as standard. The organization's employees and subcontractors have access to information resources only to the extent necessary for the performance of their work.
All employees and subcontractors are subject to professional confidentiality for an indefinite period. In other words, official confidentiality continues to apply even after the end of their contract.

8.2.7 Relations with third parties

The relationships between the SOPHiA GENETICS, its customers and its sub-processors, are governed by appropriate assessments and agreements defining the responsibilities of the parties in the data processing. Between the Data Processor and its sub-processor additional responsibilities and guarantees are added.

8.2.8 Auditing

SOPHiA GENETICS conducts regular internal audits to ensure our processes, infrastructure, and systems align with industry best practices and our stringent internal policies. Additionally, our organization is audited by an independent external certification body to uphold compliance with

ISO 27001:2022 (Information Security Management), ISO 27017:2015 (Cloud Security), and ISO 27018:2019 (Protection of Personally Identifiable Information in the Cloud) standards.

9 Return, transfer and disposal of data

9.1 Data retention and deletion

Upon signing the contract, customers receive five years of access to our platform. During this time, all Customer Data will be securely retained. For customers dealing with regulated product, we comply with specific laws and regulations that may necessitate retaining such information for up to ten years.

Files uploaded for analysis—such as FASTQ, BAM, and VCF files—will remain in our active database for a maximum of 90 days to facilitate troubleshooting. After this period, these files will be archived, as they are no longer required for processing. Should customers need to retrieve any archived files, they can easily do so by contacting our customer service team.

This retention schedule for data in the SOPHiA DDM™ and cloud service ensures that our customer data are retained and remain accessible while adhering to necessary compliance regulations.

9.2 Assets end-of-life

At the end of an asset's life, whether physical or logical, the Security Manager of SOPHiA GENETICS is responsible for ensuring that it is permanently destroyed, and that it cannot leak confidential information. For example, computer files must be permanently destroyed, computer equipment at the end of its life must be entrusted to a company specialized in destruction and certified ISO 9001, and physical documents must be destroyed via the document shredder present in SOPHiA GENETICS' office.

10 Customer contribution to security

We invite our valued customers to prioritize the security of their data and systems as they utilize our SOPHiA DDM™ platform for analyzing sensitive healthcare information. To ensure the protection of your data and compliance with regulatory standards, we recommend implementing the following security measures:

Access Control

- Ensure you identify users who will be granted access to the platform and regularly update access rights by contacting SOPHiA GENETICS support service.
- Ensure strong user authentication by implementing multi-factor authentication (MFA) and role-based access control (RBAC) to limit access to sensitive information based on job responsibilities.
- Implement complex password, using an arbitrary combination of numbers, symbols and upper- and lower-case letters. Raise awareness among your employees to ensure they don't share their password with others for accessing to the platform.

Data protection

- Prior to uploading or inputing data into the platform ensure you have the right authorization and consent to do so. While the SOPHiA DDM™ platform allows the user to complete multiple fields for convenience, few fields are compulsory. Please ensure your apply data minimization requirements and follow your internal rules and policies.

- Ensure compliance with your local data protection regulations, conducting regular audits and risk assessments to identify and mitigate vulnerabilities.

Network Security
Make sure you have implemented appropriate firewalls to secure your internal network and utilize virtual private networks (VPNs) for secure remote access. Many firewalls will automatically monitor Internet activity and give a warning if there's a problem. Several products on the market combine anti-virus and personal firewall functionalities. Verify that it is permanently activated and updated.

Endpoint Security
Install and regularly update antivirus and anti-malware software on all devices accessing our platform. Establish a robust patch management process to protect against vulnerabilities.

Employee Training and Awareness
Provide ongoing security awareness training for staff to help them recognize and respond to potential threats, including phishing attempts and social engineering attacks.

Physical Security
Implement physical access controls and use surveillance systems to monitor spaces where patient data is processed or stored. Remind users to lock their computers when unattended to prevent unauthorized access

Monitoring and Logging
Utilize security information and event management (SIEM) solutions to monitor and analyze security events in real time, and maintain access logs to track user activity.

By adopting these security measures, you can significantly enhance your organization's ability to protect patient data and mitigate risks associated with data analysis. We are here to support you in implementing these measures and ensuring the secure use of our platform.
If you have any questions or need assistance with specific security practices, please feel free to reach out to our support team.

Annex I - LIST OF INFORMATION SECURITY DOCUMENTS

Type of document	Title
Certificate of Registration	ISO/IEC 27001:2022 - Information Security Management System
Certificate of Registration	ISO/IEC 27017:2015 - ISMS Cloud Security
Certificate of Registration	ISO/IEC 27018:2019 - Management System for Protection of PII in Public Clouds acting as PII Processors
Policies & procedures	Information Security Governance Policy
Policies & procedures	Information Security Management Manual Policy
Policies & procedures	General Policy on Personal Data Protection
Policies & procedures	Access Management Policy
Policies & procedures	Asset Management Policy
Policies & procedures	Availability Management Policy
Policies & procedures	Backup Policy
Policies & procedures	Business Continuity Management
Policies & procedures	Communication and Network Management Policy
Policies & procedures	Disaster recovery policies
Policies & procedures	Data Transfer Policy
Policies & procedures	Cryptographic Policy
Policies & procedures	Records Retention and Disposal
Policies & procedures	Security Incident Management Policy
Policies & procedures	Secure Guidelines for Software Development Policy
Policies & procedures	Software Development Lifecycle (SDLC)
Policies & procedures	Vulnerability Management Policy
Policies & procedures	Confidentiality Statement
Policies & procedures	Acceptable Use of Information Systems Policy
Policies & procedures	Physical and Environmental Security Policy