AYADATA

Technical and Organizational Security Measures

Providing and maintaining the security and safety of personal and/or special category data belonging to the individuals/entities we deal with is paramount to our company ethos. Aya Data adheres to the GDPR and SOC 2 with its associated principles in every process and function. With developed policies, procedures, controls, and measures, Aya Data ensures maximum and continuous compliance with the GDPR and SOC 2 principles, including staff training, procedure documentation, audit measures, and assessments.

Aya Data proudly operates a "Privacy by Composition" approach, which intends to be proactive, not reactive; evaluating changes and their impact from the onset and designing systems and methods to safeguard personal data is at the core of our business and employee culture.

1. Confidentiality and Non-Disclosure Agreements (NDAs)

All levels of employees, board members, investors, and contractors are fully informed about their roles concerning data protection, which are bound by secrecy and confidentiality. Moreover, they have signed a Confidentiality Agreement and/or Non-Disclosure Agreement which is held on file as per our Confidentiality and Non-Disclosure Policy. With the application of our data classification policy, every data utilized in the organization is classified according to the appropriate level of confidentiality accorded to it from the onset. Confidentiality levels are classified as public, internal use, restricted, and confidential, with access granted respectively to the employee's level of clearance.

Aya Data does not access, use, or share Client Data to any third party, except when this access, use, or sharing is necessitated by providing the Services or as a requirement to comply with law enforcement or regulators requests.

2. Employee Background Checks

- Once accepted into the business based on testing, interviews and screening, all prospective employees of Aya Data are required to submit a recent drugs test / medical report, a police report (showing no previous record), proof of right to work in the relevant market, passport / ID and two references from previous employment or academic study.

3. Physical Security

To maintain Physical Office Security and protect persons and equipment within its premises, Aya Data ensures the following, but is not limited to:

i. A standard building with office space to accommodate and house personnel and equipment to facilitate a smooth working environment per the business objectives, laws, and regulations as best international practices.

ii. Security areas are provisioned in layers by designating different security zones within the building. Security zones include areas designated as Public, Private, and Special Access.

iii. Security personnel is on-site.

iv. CCTV cameras

v. Access control mechanisms

vi. Employees photo identification cards

vii. Furthermore, information processing offices handling confidential data are strategically located to minimize information exposure to unauthorized persons during their use. Proper records are also kept on the movement of persons entering or exiting the facility, and adequate mechanisms are well placed to mitigate potential physical and environmental threats.

4. Access Control

- To protect privileged access to Aya data assets and resources, Aya Data deploys various access control mechanisms suitable for multiple levels of information access across the organization to stand against deliberate and unintentional risk. This includes but is not limited to:

  Physical, Network, Workstation, and Password access control mechanisms as per our privacy protection policy and Data protection and security policy.

  i. Physical access control mechanisms such as CCTV cameras and Key access & card systems are in place to regulate and monitor the movement and activities of persons accessing the building and particular areas within the building. Key or access key cards are given to employees and contractors depending on individual job descriptions and provided by Human Resources, who keep appropriate records. Key movement logs and record books are kept to track all persons in/out activities.

  ii. Network access covers controls to secure and protect Aya Data's network. The network is regulated by the DPO and network administrator only. As per our Data protection and security policy, our network is secured and continuously monitored with state-of-the-art firewall devices, anti-virus and malware software, and EDR tools. All connections are secured with 256-bit end-to-end encryption. Remote conations to our systems utilize only Aya data's approved VPN. Access to network devices and configurations are strictly restricted to authorized persons only.

  iii. Workstation: Aya Data Ltd executes physical and technical protection for all workstations that access electronic confidential data to regulate access to accredited users. Appropriate standards include: Limiting physical access to workstations to only authorized personnel while enabling a password-protected screen saver with a shorter timeout period, guaranteeing the protection of workstations left unattended. With the deployment of endpoint security, all workstations are safeguarded against malicious actors and campaigns.

5. Data Security

- Data security covers control of data security at rest, in transit, and via authorized access mechanisms. This includes obtaining, classifying, protecting, and monitoring sensitive data assets using access control, encryption, and logging.

- As Aya Data processes personal information regarding individuals (data subjects), we are obligated under the GDPR and SOC 2 regulations to safeguard such information, and to obtain, use, process, store and destroy it, only in concession with the GDPR and SOC 2 principles.

- Aya Data ensures that even more excellent care and attention is given to personal data falling within the GDPR's 'special categories' (previously referred to under the DPA as sensitive personal data). For the assumption that this type of information could be used in a harmful or discriminatory way and is of a sensitive, private nature to the people it refers to.

- As Aya Data uses personal data in one or more of the above capacities, we have put robust measures, policies, procedures, and controls concerning all aspects of general data handling.

6. Isolation Control:

- Aya Data employs various Isolation controls suitable for multiple forms of risk. Our policy is to Isolate systems storing or processing sensitive information and separate compromised systems from the main network until confirmed to be clean.

- For development, test, and production environments, separate subscriptions, management groups, or both are implemented. Applications that process sensitive information are isolated from other apps in the same manner when needed using a Virtual Network. Further techniques such as network security groups and subnets for application isolation may be utilized.

- Physical and Logical isolation is deployed to segregate each client's applications and data where applicable.

- Generally, our installed firewall device isolates Aya Data systems from the rest of the world

7. Pseudonymization:

- Using techniques such as aggregation, elimination, and identifier range, Aya Data processes personal data for secondary use, employing Anonymization and Pseudonymization in a way that the data cannot be linked to a particular Data Subject without the aid of additional information, kept separately.

8. Availability Control:

To minimize the amount of unforeseen or unplanned downtime (also called outages) of information systems under Aya Data Ltd.’s control, various methods have been employed, such as:

- Physical: redundant storage, network, and power mitigate hardware issues that could lead to data unavailability or loss.
- Logical: firewall devices and configuration provides reliable systems isolation. Online and offline backups are kept to prevent accidental or intentional destruction or loss.
- Rapid recovery: In the case of a physical or technical incident, Aya Data preserves the ability to promptly reinstate the availability and access to personal data. Appropriate measures are in place for incidents to be identified, contained, investigated, resolved, and information related to the breach communicated with the relevant entities.

9. Order Control:

Data processors from Aya Data are subjected to clear and unambiguous contractual or order agreements, formalized order management, stringent controls on the selection of the Service Provider, as well as frequent supervisory follow-up checks from senior management to ensure progress tracking and fulfilment of contractual agreements.

10. Data Transfer Control:

- As per our Data transfer policy, electronic data and storage media is only transferred in an encrypted form. On the other hand, paper documents are only transmitted by a reliable person or courier in a sealed envelope to ensure that no unauthorized reading, copying, changes, or deletion happen during the transfer.

12. Internet Access Security

Access to the organization’s internet is regulated by the DPO and network administrator only. As per our Data protection and security policy, our network is secured and continuously monitored with state-of-the-art firewall devices, anti-virus and malware software, and EDR tools. All connections are secured with 256-bit end-to-end encryption. Remote conations to our systems utilize only Aya data's approved VPN. Access to network devices and configurations are strictly restricted to authorized persons only.

13. Awareness Programs

- Aya Data uses several methods to impart training and development to keep up with technological evolvement and employee development. To keep employees, board members, investors, and contractors abreast with current trends, training activities are usually delivered in a blend of the following forms:
  - i. Formal training (individual or corporate).
  - ii. Training presented by internal and/or external experts.
  - iii. On-the-job training (OJT).
  - iv. E-learning.

v. Conferences/Seminars participation.
vi. Rotation assignments.
vii. Pre-employment training.
viii. Training apprentices.
ix. Employee coaching and mentoring.
x. Job shadowing.

14. Tolerance Policy

- A vital part of Aya data's information security program is a comprehensive and systematic approach to risk management. The process is made up of four parts: identification of the organization's assets, along with the threats and vulnerabilities that apply; evaluation of the likelihood and consequence (risk) of the threats and vulnerabilities being recognized; identification of treatment for each intolerable risk; and evaluation of the residual risk after treatment.
- Aya Data operates with five (5) risk tolerance level descriptions: Very low; Low; Moderate; High, and Very High. Risk assessment results with very low and low levels are tolerable levels per Aya data's Risk assessment Policy. In contrast, results tagged with Moderate, High, and Very High must be treated to uphold data security, confidentiality, integrity, and availability.