DATA PROTECTION STATEMENT

1) OVERVIEW

Neurozone manages information of various customers. Neurozone understands that its customers expect Neurozone to protect their information with the highest standards and are committed to providing them with a highly secure and reliable environment.

2) TECHNOLOGICAL MEASUREMENTS

Our security model and controls are based on international standards and industry best practices, such as ISO 27001, ISO 27018 and OWASP Top 10.

a) How does Neurozone secure its customer's information?

i) Our systems are hosted in multiple hosting environments: Google Cloud and Microsoft Azure. These services can be re-deployed within 30 minutes and all databases are backed up on a weekly basis. This allows Neurozone to provide a reliable service and keeps the customer information available whenever the customers need it. Neurozone does not have a disaster recovery site at the moment, this will be implemented in the future.

ii) These data centres employ leading physical and environmental security measures, resulting in highly resilient infrastructure. For more information about their security practices, see below:

(1) Google Cloud Security

(2) Microsoft Azure Security

iii) Subcontractor services that are used for data processing and analytics (i.e. Matogen Applied Insights (Pty) Ltd) are strictly POPIA/GDPR compliant.

b) Application Security

i) Neurozone implements a security-oriented design in multiple layers, one of which is the application layer. The Neurozone application is developed according to the OWASP Top 10 framework and critical code is peer-reviewed prior to deployment to production.

ii) Neurozone's controlled CI/CD process includes static code analysis, vulnerability assessment, end-to-end testing, and unit testing which addresses authorization aspects. Security training is not yet provided to Neurozone developers.

c) API access

All actions called against the Neurozone API, use:

i) SSL/TLS (HTTPS) for transmission layer security.

ii) An authentication header for every request using a securely generated bearer token supplied by Google's Firebase authentication service.

iii) All API Access is restricted to the roles allocated to the user, for non-admin roles access is restricted to the user's own data as well as non-user specific data.

d) Infrastructure and Operational Security

Another layer of security is the infrastructure. As stated, Neurozone is hosted across multiple Google Cloud and Microsoft Azure Zones. Furthermore, our infrastructure is protected using multiple layers of defence mechanisms, including:

i) Only serverless services are used and, excluding the API, all of these services are configured to be restricted to inter-service level authentication mechanisms.

ii) All serverless services only accept HTTP traffic and all other ports are closed.

iii) No root access is provided to serverless services to any users.
iv) Firewalls for enforcing IP whitelisting and access through permitted ports only to Matogen network resources.
v) Only Senior Engineers use provisioned SSH keys for infrastructure administration access.
vi) Only senior staff that administer services are granted access.

e) Data Encryption

Neurozone encrypts all data both in transit and at rest:

i) All data stored is encrypted at rest with AES encryption and the encryption keys themselves are encrypted with a set of regularly rotating master keys.
ii) External traffic is encrypted using TLS 1.3 with a modern cipher suite, supporting TLS 1.2 at minimum;
iii) Internal traffic is encrypted with Application Layer Transport Security (ALTS) as per Google Cloud's standard inter-service security;
iv) User data is encrypted at rest across our infrastructure using [AES-256] or better;
v) User credentials use Google's provided Firebase Authentication authentication service and no credentials are stored in any of the Neurozone services.
vi) Non-Google service credentials are encrypted using Google's KMS service which uses AES-256 encryption.

f) External Security Audits and Penetration Tests

i) There are currently no external audits or independent penetration tests, this will be carried out in the future.

g) Physical Security

i) Neurozone is a cloud-based company, with no part of our solution infrastructure retained on-premise.
ii) Neurozone's data centres are hosted on Google Workspace, Mixpanel, and OneSignal infrastructure, where leading physical security measures are employed.

h) Disaster Recovery and Backups

Neurozone is committed to providing continuous and uninterrupted service to all its customers. Neurozone consistently backs up user data 3 times a week. All backups are encrypted and retained for 365 days.
Neurozone does not yet have a Disaster Recovery & Business Continuity Plan.

i) Security Awareness and Training

Neurozone understands that its security is dependent on its employees and has therefore implemented a clean desk and clear screen policy. Customer data is not stored locally on any devices. However, employees do not yet receive regular information and security awareness training.

j) Access Control

i) Solutions:

(1) Authorised User activation centralised.
(2) Authorised Users activated only on instructions from customers.
(3) Neurozone knows the information the Customer uploads to Neurozone's solutions/services is processed as private and confidential information.
(4) Neurozone regularly conducts user access reviews to ensure appropriate permissions are in place, in accordance with the least privilege principle. Employees have their access rights promptly modified upon change in employment.

ii) Internal:

Remote Access policy and procedures implemented and communicated to all personnel.

3) ORGANISATIONAL MEASUREMENTS

Neurozone have established and are maintaining the following organisational measurements:

a) Governance:

i) Appointed an Information Officer;
ii) Registered the Information Officer with the information Regulator;
iii) Established and rolling out a Privacy Management Accountability Framework focussing on the following categories:
  (1) Governance Structure;
  (2) Maintain personal Information inventory and data transfer mechanism;
  (3) Maintain internal Data Protection policy;
  (4) Embedded Data Privacy into Operations;
  (5) Training and Awareness programs;
  (6) Manage Information Security Risks;
  (7) Manage Third Party Risks;
  (8) Maintain Notices (to address Openness condition under the POPIA);
  (9) Respond to request and complaints from third parties;
  (10)Monitor and evaluate operational practices;
  (11)Maintain Data Privacy Breach Management Program;
  (12)Monitor Data Handling Practices; and
  (13)Track external compliance requirements and best practices.

b) Privacy Impact Assessment executed at Neurozone and PIAs execute on any new projects

c) Employees:

i) Employee and independent contractor agreements to confirm Customer Data (including Personal information) as Confidential Information;
ii) Implementation and roll out of the following policies:
  (1) NEUROZONE Mobile Devices Policy,
  (2) NEUROZONE's IT Security Policy,
  (3) NEUROZONE's Data Protection Policy,
  (4) Electronic information and Communication System Policy,
  (5) Incident Management Policy and Procedures, and
  (6) Direct Marketing Policy.
iii) Processing of Personal information awareness campaigns
iv) Privacy training with employees and contractors do not occur as yet, but the implementation of training will take place on a semi-annual basis.

d) Customer Engagement:

i) eMail legal notice reflected on each email, incorporating by reference the Neurozone Privacy Policy;
ii) Neurozone Privacy Policy is available to all Customers and users of the Neurozone websites and Services;
iii) Updated General Terms and Conditions with appropriate Processing of Personal Information provisions;
iv) Updated Software as a Services Agreement with appropriate Processing of Personal Information provisions.

e) **Third Party Service Provider Engagements:-**

i) Identified all third party Operators;
ii) Written Agreements with 3rd Party Operators; and
iii) Evaluation of third party Data Protection Statements and/or Privacy Practices.