Information Security Overview

Last Updated: December 31 2018

Nipendo Ltd. ("**Company**" or "**we**") is committed to provide transparency regarding the security measures which it has implemented in order to secure and protect Personal Data (as defined under applicable data protection law, including without limitations, the EU General Data Protection Regulation ("**GDPR**") and the upcoming California Consumer Privacy Act ("**CCPA**") (collectively "**Data Protection Regulation**") processed by the Company for the purpose of providing its services.

This information security policy outlines the Company's security, technical and organizational practices.

As part of our data protection compliance process we have implemented technical, physical and administrative security measures to protect the Personal Data, including upholding standards of ISO 27001 and SOC 2 Type II.

Physical Access Control
The Company ensures the protection of the physical access to the data servers which store the Personal Data for The Company. The data processed by the Company are stored either in Company's local server farm, or in the IBM SoftLayer and Microsoft Azure data servers. Further, the Company secures the physical access to its offices to ensure that solely authorized individuals such as employees and authorized external parties (maintenance staff, visitor, etc.) can access the Company's offices.

System Control
Access to the Company's database is highly restricted in order to ensure that solely the appropriate prior approved personnel can access the Company's database. Safeguards related to remote access and wireless computing capabilities are in implemented therein. Employee are assigned private passwords that allows strict access or use related to Personal Data all in accordance with position, and solely to the extent such access or use is required. There is constant monitoring of the access to the data and the passwords used to gain login access.

Data Access Control
There are restrictions in place in order to ensure that the access to the Personal Data is restricted to employees which have a permission to access it, all in order to ensure that Personal Data shall not be accessed, modified, copied, used, transferred or deleted without specific authorization. The access to the Personal Data, as well as any action performed involving the use of the Personal Data requires a password and user name, which is routinely changed, as well as blocked when applicable. The user password is fully encrypted. Each employee is able to perform actions solely according to the permissions determined by the Company. Each access is logged and monitored, and any unauthorized access is automatically reported. Further, the Company has ongoing review of which employees' have authorizations, to assess whether access is still required. Company revokes access immediately upon termination of employment. Authorized individuals can solely access Personal Data that is established in their individual profiles.

Organizational and Operational Security
The Company invests a multitude of efforts and resources in order to ensure compliance with the Company's security practices, as well as continuously provides employees training. The

Company strives to raise awareness to the risk involved in the processing of Personal Data. In addition, the Company implemented applicable safeguards for its hardware and software, including firewalls and anti-virus software on applicable Company hardware and software, in order to protect against malicious software.

Transfer Control

The Company does not transfer any Personal Data outside of the Company's cloud servers. All transfer of Personal Data between the client side and the Company's servers is protected using encryption safeguards such as L2TP, IPsec (or equivalent protection), as well as encryption of the Personal Data prior to the transfer of any Personal Data. The Company's servers are protected by industry best standards including the EU-US privacy shield framework. Furthermore, the destruction of Personal Data following termination of the engagement is included within the contract between the parties. In addition, to the extent applicable, the Company's business partners execute an applicable Data Processing Agreement, all in accordance with applicable laws.

Availability Control

The Company's servers include an automated backup procedure on a daily basis.

Data Retention

Personal Data are retained for as long as needed to provide the services or as required under applicable laws. Individuals may request data deletion, however this request is not absolute and is limited, all as detailed in the Company Data Subject Overview.

Job Control

All of the Company's employees are required to execute an employment agreement which includes confidentiality provisions as well as applicable provisions binding them to comply with applicable data security practices. In addition, employees undergo a screening process applicable per regional law. In the event of a breach of an employee's obligation or non-compliance with the Company's policies, the Company includes repercussions to ensure compliance with the Company's policies. In addition, prior to the Company's engagement with third party contractors, the Company reviews such third party's security policies, specifically their information data security policies to ensure it complies with the Company's standard for data security protection. Third party contractors may solely access the Personal Data as explicitly instructed by the Company.