ONGAGE SECURITY POLICY

(Last modified: July 19, 2021)

Ongage Ltd. ("**Company**" or "**we**") is committed to provide transparency regarding the security measures which 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 California Consumer Privacy Act ("**CCPA**") (collectively "**Data Protection Regulation**") processed by the Company for the purpose of providing its services.

This 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 our customers' and customer's users' Personal Data as explained below.

The security objectives of the Company are identified and managed to maintain a high level of security and consists of the following (concerning all data assets and systems):

- **Availability** - information and associated assets should be accessible to authorized users when required. The computer network must be resilient. The Company must detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information.
- **Confidentiality** - ensuring that information is only accessible to those authorized to access it, on a need-to-know-basis.
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorized modification, of electronic data.

Physical Access Control

The Company ensures the protection of the data servers which store the Personal Data for the Company from unwanted physical access.

The Personal Data that is processed by the Company and which the Company is the Controller of (as such term is defined under the GDPR) is stored on Amazon Web Services.

The data processed by the Company as a Processor (as such term is defined under the GDPR) may be stored on Amazon Web Services (AWS),. Please see AWS's security measures here. The Company also secures physical access to its offices by ensuring that only authorized individuals such as employees and authorized external parties (maintenance staff, visitors, etc.) can access the Company's offices by using security locks and an alarm system, amongst other measures as well.

System Control

Access to the Company's database is highly restricted in order to ensure that only the relevant personnel who have received prior approval can access the database. The Company has also

implemented appropriate safeguards related to remote access and wireless computing capabilities. Employees are assigned private passwords that allow strict access or use to Personal Data, all in accordance with such employee's position, and solely to the extent such access or use is required. There is constant monitoring of access to the Personal Data and the passwords used to gain access. The Company is using automated tools to identify non-human login attempts and rate-limiting login attempts to minimize the risk of a brute force attack.

Data Access Control

User authentication measures have been put in place in order to ensure that access to Personal Data is restricted solely to those employees who have been given permission to access it and to ensure that the Personal Data is not accessed, modified, copied, used, transferred or deleted without specific authorization for such actions to be done. Any access to Personal Data, as well as any action performed involving the use of Personal Data requires a password and user name, which is routinely changed, as well as blocked when applicable. Each employee is able to perform actions solely in accordance with the permissions granted to him by the Company. Furthermore, the Company conducts ongoing reviews of the employees who have been given authorization to access Personal Data, in order to assess whether such access is still required. The Company revokes access to Personal Data immediately upon termination of employment. Authorized individuals can only access Personal Data that are located in their individual profiles.

Organizational and Operational Security

The Company puts a lot of effort and invests a lot of resources into ensuring that the Company's security policies and practices are being complied with, including by continuously providing employees with training with respect to such security policies and practices. The Company strives to raise awareness regarding the risks involved in the processing of Personal Data. In addition, the Company has implemented applicable safeguards for its hardware and software, including by installing firewalls and anti-virus software on applicable Company hardware and software, in order to protect against malicious software.

Transfer Control

All transfers of Personal Data between the client, the Company's service providers and the Company's servers are protected by the use of encryption safeguards, including the encryption of the Personal Data prior to the transfer of any Personal Data.. In addition, to the extent applicable, the Company's business partners execute an applicable Data Processing Agreement, all in accordance with applicable laws.

Input Control

The Company ensures the transparency of input controls, including changing and the deletion of data.

Availability Control

The Company maintains backup policies and associated measures. Such backup policies include permanent monitoring of operational parameters as relevant to the backup operations.

Furthermore, the Company's servers include an automated backup procedure. The Company also conducts regular controls of the condition and labelling of data storage devices for data security. The Company ensures that regular checks are carried out to determine whether it is possible to undo the backup, as required and applicable.

International Transfer

On July 16, 2020, Europe's highest court ("**CJEU"**) invalidated the EU-US Privacy Shield. Additionally, on September 8, 2020, the Swiss Data Protection Authority announced in a position statement that it no longer considers the Swiss-U.S. Privacy Shield adequate for the purposes of transfers of personal data from Switzerland to the U.S.

We ensure any data transfer is done in a secure manner, in compliance with the latest EDPB recommendations concerning data transfer as well as contractually sign a Data Processing Agreement which incorporate the Standard Contractual Clauses which remain a valid data export mechanism and which automatically apply in accordance our Data Processing Agreement.

Over the coming months, we anticipate that EU data protection regulators will issue additional guidance on the CJEU decision, including what the supplementary measures could consist of for those transferring data in reliance on the SCCs. In addition, the current form of the SCC was written before the GDPR went into effect and will be updated at some point in time. We will continue to keep a close eye on forthcoming guidance to stay up to date and assess whether we need to make any changes to our existing practices.

Data Retention

Personal Data is retained for as long as needed for us to provide our services or as required under applicable laws.

Job Control and Third Party Contractors and Service Providers

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 the event of a breach of an employee's obligation or non-compliance with the Company's policies, the Company implements certain repercussions in order to ensure compliance with the Company's policies. In addition, prior to the Company's engagement with third party contractors, the Company undertakes diligence reviews of such third party contractors. The Company agrees with third party contractors on effective rights of control with respect to any Personal Data processed on behalf of the Company. The Company ensures that it enters into data protection agreements with all of its clients and service providers.

Penetration Testing

External penetration test is performed on an annual basis. The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing

confidential information other than their own. The penetration tests and security scans are performed by a reputable Third-party vendor. In addition, The Company conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment. Actions are taken to remediate identified deficiencies on a timely basis. Vulnerability scans is performed using external tools, in order to detect potential security breaches

Compliance Programs

Ongage operations, policies and procedures are audited regularly to ensure Ongage meets all standards expected as a cloud system provider. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. Ongage's systems and services were audited and verified by ISO 27001.

Ongage's customers remain responsible for complying with applicable compliance laws, regulations and privacy programs in addition to Ongage's compliance with privacy and security regulations.

Reporting a security issue

Ongage is exerting considerable resources to ensure a secure code and infrastructure for all of its products. If you believe that you have found a security vulnerability in any of our products, please report it to us straight away via e-mail to info@ongage.com. Please be sure to include a brief description, detailed steps to reproduce and what might be the impact.

Responsible disclosure policy

We encourage responsible disclosure, and we promise to investigate all legitimate reports and fix any issues as soon as we can. We ask that during your research you make every effort to maintain the integrity of our any data you come across, avoiding violating the privacy of any person or degrading our offerings. Please provide Ongage reasonable time to fix any vulnerability you find before you make it public. In return we promise to investigate reports promptly and not to take any legal action against you.