# TECHNICAL AND ORGANIZATIONAL MEASURES

The Company is committed to undertaking all the required and relevant technical measures aimed at optimal personal data protection, in relation to all categories of data that are within its control or reach, in its capacity of controller as well as in its capacity of processor.

## Data anonymization

Processing of the personal data of the clients' web sites visitors is conducted in the following manner: (i) all web site visitors' personal data used, i.e. IP addresses and cookie identifiers, are immediately, in the first step of processing, rendered anonymous in such a manner that the data subjects are no longer identifiable, so that system further processes only anonymized data, while (2) raw personal data of clients' web sites visitors are stored for the purpose of possible re-processing for a period of maximum 7 days.

## Host Management and Security

All Company's cloud servers are Linux servers, which are regularly patched and upgraded.

Servers are behind a virtual private cloud networking setup.

Because the Company relies on public cloud infrastructure, physical security of our data centers are handled by respective cloud service provider, who has public documentation on cloud security, as well as compliance for their infrastructure.

The Company is actively monitoring for unusual behavior and dedicated team members receive automatic notifications for suspicious activities.

The Company employs industry best practices firewall configuration as well as active protection against attacks with banning policies.

## System monitoring, logging, and alerting

The Company uses centralized log collection and analysis for security, system and application monitoring, availability, access, and other metrics about the services.

Logs are analyzed for security events via automated monitoring software, overseen by the team members.

## Data transfer encryption and at rest

All Company's application and API endpoints are TLS/SSL only.

The Company monitors the changing cryptographic landscape and upgrade the cipher suite choices as the landscape changes, while also balancing the need for compatibility with older clients.

Data at rest in production network is encrypted. This applies to all types of data at rest within the system (file stores, databases, backups, etc.)

## Personnel Practices

The Company has established a procedure to ensure that system access is revoked for persons whose employment has been terminated. The procedure also establishes appropriate responsibilities when a termination occurs.

The Company monitors and maintains an audit log of all access to the system.

The Company uses Two-Factor Authentication for all users in the organization on all services where possible.

## System Security Testing, Evaluation Plans and Procedures

The Company has implemented the process for regularly testing, assessing and evaluating the effectiveness of technical measures for ensuring the security of processing.

# ORGANIZATIONAL MEASURES

## Confidentiality

The Company has a practice of signing confidentiality agreements with all its employees, outsourced staff or partners that have any access to personal data it processes.

Agreements with the outsourced staff that have the position of the sub-processors contain all the relevant and required personal data protection clauses as required by the GDPR or other applicable laws.

## Limited access measures

Access to Company's systems and any personal data is restricted only to needed team members in order to perform their respective tasks and obligations.

## Appointment of DPO

Although the Company is not legally obliged to do so, as a part of its efforts to implement best practices in personal data protection handling, the Company shall appoint a Data Protection Officer (DPO).

DPO’s contact details shall be available on the Company's web site.

## Raising Awareness and Internal Trainings

The Company's management is dedicated to continual raising of awareness within the Company on the relevance and importance of careful, legal and proper personal data handling. For this purpose, regular trainings shall be held for all Company's employees and staff or smaller teams or team members, as appropriate and/or required by DPO.

All new employees or staff members shall be acquainted with this policy, all other relevant internal documents and procedures, and where required, trained in order to act in accordance with those.

## Disciplinary Consequences

All Company's employees or staff members shall be held accountable for their acts and omissions related to inappropriate personal data handling, and shall bear proportionate disciplinary and/or other consequences, including termination of employment or cooperation agreement.