**Policy Statement**

**General Statements**

The Company fully complies with GDPR requirements and is able to demonstrate the proof.

The Company shall take all possible measures to protect personal data belonging to EU data subjects that the Company might process in the course of its activities.

The Company claims that personal data belonging to EU data subjects that the Company might process in the course of its activities:

1. shall be processed lawfully, and the lawfulness of processing shall be verified;
2. shall be processed fairly and in a transparent manner in relation to the data subject;
3. shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
4. shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
5. shall be accurate and, where necessary, kept up to date;
6. shall be kept no longer than is necessary for the purposes for which the personal data are processed or no longer than the applicable legislation requires;
7. shall be protected from unauthorized or unlawful use or processing, disclosure, loss, destruction or damage by means of technical and organizational measures selected in accordance with the risk-based approach.

The Company claims to ensure that the basic rights of a data subject shall be preserved: right of access, right to rectification and erasure, right of restriction of processing, right to data portability, right to object, right not to be subject to a decision based solely on automated processing.

**Confidentiality**

The Company ensures that its employees and any persons under its authority who access the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**Data Processing Agreements**

Where it is required to transfer personal data belonging to EU data subjects to a third country, Data Processing Agreement (hereinafter referred to as DPA) shall be signed between the parties involved.

The Company shall process the personal data following the requirements stipulated in DPA signed.

**Technical and Organizational Measures**

The Company claims to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

The Company claims to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

The Company claims to ensure that personal data is protected from unauthorized or unlawful use or processing, disclosure, loss, destruction or damage and processing is performed in accordance with this Regulation.

For the following purposes, the Company has implemented appropriate technical and organizational measures (hereinafter referred to as TOMs) [link]

* TOMs have been selected and implemented based on the risks defined in the course of the personal data processing risk analysis.
* TOMs might be implemented following customers’ requirements.
* TOMs shall be reviewed and updated on a regular basis in accordance with [link].

**Technical and Organizational Measures Effectiveness Review**

TOMs shall be audited and reviewed for effectiveness in the course of internal audits and the results shall be kept [link].

**Personal data Inventory**

The inventory of personal data processed by the Company shall be kept along with the lawful ground for processing [link].

**Personnel Authorized to Process Personal Data**

The list of the personnel authorized to process personal data shall be kept [link].

**Personal Data Processing Rules Awareness**

The personnel of the Company is obliged to take appropriate training in regard to personal data processing rules adopted in the Company. The training materials and records shall be kept [link].

**personal data breach Notification Procedure**

In the event of a personal data breach, the Company shall follow the data breach notification process:

* Supervisory authority shall be notified: where feasible, not later than 72 hours.
* Data subject shall be notified
* Personal data breaches shall be documented, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

**Code of Conduct**

Code of conduct has been adopted in the Company for the purpose of specifying the application of GDPR in the Company [link].