**APPROVED:**

STNK UAB

By the order of the Director dated January 6, 2025, No. 2025-701-1

**STNK, UAB**

**PERSONAL DATA PROTECTION POLICY No. 2025-702-1**

**Definition of Terms**

**Company** – STNK, UAB, legal entity code 306995317, registered office address: Skroblų g. 12-152, Vilnius.

**Employee** – a person employed by the company under an employment contract.

**Manager** – the director of the company.

**Personal data** – any information related to a natural person whose identity is known or can be directly or indirectly determined using such data as a personal code, one or more characteristics of physical, physiological, psychological, economic, cultural or social nature.

**Policy** – this Personal Data Protection Policy.

**Purpose and Scope**

The Personal Data Protection Policy is prepared and applied to protect the company's employees, partners, and clients from unlawful and harmful direct or indirect, intentional or unintentional actions of individuals in handling personal data accessible to them, as well as using appropriate equipment for performing their work functions.

The Policy must be applied within the company when processing personal data in any systems or on any media, regardless of whether the processing is related to internal business operations or external relations with any third parties. It also applies to employees using the provided equipment and tools during the performance of their duties.

Any data that can be considered personal data and becomes accessible or known to employees in the course of their duties is deemed confidential company information and must be protected and not disclosed to other employees or third parties, except those authorized to access such data under the company’s procedures. The company specifies that such data must be protected regardless of the form in which it is obtained (printed, on a storage device, audio/video format, etc.).

**Employee Responsibilities**

All personal data and other identifying information must be collected and processed only when necessary, and only to the extent required for the employee to perform their functions within the scope of their authority and in compliance with applicable data protection laws, particularly Regulation (EU) 2016/679 of April 27, 2016 (General Data Protection Regulation – GDPR).

Personal data encountered during work must be treated as confidential and protected according to this Policy; it may not be disclosed without legal grounds. An employee unsure whether they are authorized to disclose data must contact the manager or designated person for confirmation.

Every employee must comply with this Policy and all applicable laws and rules regarding the collection, storage, and processing of personal data. Breach of this Policy will be considered a serious misconduct and may result in disciplinary action or termination. The employee may also face administrative or criminal liability.

**Use of Computer Systems**

Any computer devices and electronic databases are accessible to employees based on their job responsibilities and according to the 'need to know' principle. Access to a database does not imply authorization to view or use all information in it.

The company may use user IDs that are unique and identify specific employees. Each employee is responsible for all actions performed under their ID account. IDs must not be shared with third parties, including other employees, unless otherwise specified by the company.

Passwords protecting computer systems and databases must be created responsibly – hard to guess, not containing personal data, and regularly updated if needed. Each employee is personally responsible for maintaining password security and compliance with this Policy and other internal rules.

Except in specific exceptions, company-owned equipment and systems may not be used for purposes unrelated to work duties or business activities.

**Security Measures**

All personal data and related information collected and processed in any form (paper, electronic, etc.) are subject to this Policy and any legal requirements regarding collection, processing, protection, and retention. Such documents must be stored securely for the period required by law or determined by the company.

Employees are not allowed to store personal data on their own devices unless temporarily required for specific work tasks. All necessary confidential or identifiable information must be stored securely (e.g., locked files).

In compliance with applicable laws and regulations, authorized company representatives may monitor and filter employees’ internet access and online activity.

Only company-approved systems and licensed software may be installed or used on company devices. Employees must have managerial approval before downloading or installing any software.

When accessing company resources (e.g., CRM systems, email, remote databases) from personal home devices, employees must follow this Policy as if using company equipment. Storing any personal data on such devices is prohibited – processing is allowed only via company-approved online storage systems.

It is strictly forbidden to use public access devices (e.g., internet cafés, libraries, etc.) unless for urgent tasks with written permission from management.

If an employee is granted access to a client's or partner's file storage system, they must use only the tools provided by the client/partner and follow specified data security rules (e.g., encryption, password use, location restrictions, etc.).

When personal data is no longer needed for company operations, it must be deleted, all copies destroyed, and employees involved must be informed of their obligation to do so. The same applies upon termination of employment.

**Security Incident Notification**

Any security incidents or threats related to personal data processing must be reported to the manager immediately. Measures must be taken to prevent harm, resolve issues, and restore security.

If necessary, the manager must ensure that personal data security breaches are reported to authorities and affected individuals, as required by applicable laws and EU regulations.