

## DATA PROTECTION POLICY

**Last Updated May 30, 2025**

Welcome to the Data Protection Policy (the “**Policy**”) of Winzilla Ltd. (a company registered and existing under the laws of Cyprus, having registration number HE 474611 and its registered address at 39 Dimofontos Street, 3rd Floor Office 301, Nicosia, 1075, Cyprus) and its related, affiliated or subsidiary companies (the “**Company**” or “**we**”). The purpose of this Policy is to ensure that the Company complies with all applicable data protection laws and regulations and safeguards the personal data of its clients when you use the Company’s website(s) and platform(s) available at sweepking.com (the “**Site**”), as well as other related Company’s webpages, applications and products, services or content accessible through the Site (collectively the “**Services**”). The Policy also outlines the procedures for collecting, processing, storing, and disposing of personal data to ensure its confidentiality, integrity, and security.

When we refer to “you” or “your” in this Policy we mean any individual who interacts or uses our Services. By using the Services, you represent that you understand and agree to this Policy, and consent to the collection, use, and sharing of information as described in this Policy. If you do not consent to our practices, you can choose not to use the Services.

**Policy Changes.** We reserve the right to change, modify, or update this Policy by posting such changes or updates to the Services or emailing you notice of the changes. Amendments to this Policy will be posted at this URL and will be effective when posted. You can tell if this Policy has changed by checking the last modified date that appears at the top of this Policy. Your continued use of the Services following the posting of any amendment, modification or change shall constitute your acceptance thereof.

**Scope.** This Policy applies to all Company’s clients using the Services. It covers all personal data the company processes, regardless of the medium (electronic, paper, etc.) or location.

**Data Protection Principles.** The Company is committed to adhering to the following data protection principles:

(1) *Lawfulness, Fairness, and Transparency*

Personal data must be processed lawfully, fairly, and transparently regarding the data subject. The purpose of data collection and processing must be clear and communicated to the data subject.

(2) *Purpose Limitation*

Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in an incompatible manner.

(3) *Data Minimization*

Only personal data necessary for the purposes it is processed should be collected. Data collection should be adequate, relevant, and limited to necessary information.

(4) *Accuracy*

Personal data must be accurate and, where necessary, kept up to date. Inaccurate data should be corrected or deleted without delay.

(5) *Storage Limitation*

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

*(6) Integrity and Confidentiality*

Personal data must be processed to ensure its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

*(7) Accountability*

The Company is responsible for and must be able to demonstrate compliance with these data protection principles.

**How we protect your Personal Data.** We are committed to safeguarding and protecting personal data and will implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to protect any personal data provided to us from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

We provide the following safety measures regarding protection of Your Personal Identification ("PI"):

- (1) Evaluation of the effectiveness of used security measures, prior to the launch of the Site and its updates;
- (2) Establishing rules to access to personal data processed by the Site, as well as ensuring registration and recording of all actions performed with PI in the information systems of the Site;
- (3) Detection of the facts of unauthorized access to PI and the adoption of appropriate response measures.

**Legal Basis for Data Processing.** The Company will only process personal data where there is a legal basis to do so, including:

- Consent: The data subject has given clear consent to process their personal data for a specific purpose.
- Contract: The processing is necessary to perform a contract with the data subject or to take steps at the data subject's request prior to entering into a contract.
- Legal Obligation: The processing is necessary for compliance with a legal obligation to which the Company is subject.
- Legitimate Interests: The processing is necessary for the purposes of legitimate interests pursued by the Company or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

**Data Subject Rights.** Data subjects have the following rights regarding their personal data:

- Right to Access: Data subjects can request access to their personal data and obtain a copy of it.
- Right to Rectification: Data subjects can request the correction of inaccurate or incomplete personal data.
- Right to Erasure: Subject to certain conditions, data subjects have the right to request the deletion of their personal data.
- Right to Restriction of Processing: Under certain conditions, data subjects have the right to request the restriction of the processing of their personal data.

- **Right to Data Portability:** Data subjects can receive their personal data in a structured, commonly used, and machine-readable format and transfer it to another data controller.
- **Right to Object:** Data subjects have the right to object to processing their personal data in certain circumstances, including for direct marketing purposes.
- **Right to Withdraw Consent:** Data subjects can withdraw their consent to data processing anytime.

**Data Security.** The Company is committed to ensuring the security of personal data through the implementation of appropriate technical and organizational measures, including:

- **Access Control:** Limiting access to personal data to authorized personnel only.
- **Encryption:** Encrypting personal data both in transit and at rest to protect it from unauthorized access.
- **Data Anonymization:** Where possible, anonymizing personal data to reduce the risk of identification.
- **Regular Audits:** Conduct regular audits and assessments of data processing activities to ensure compliance with this policy and data protection laws.

**Data Breach Response.** In the event of a data breach, the Company will:

- **Immediate Action:** Take immediate steps to contain and mitigate the breach.
- **Communication:** Inform the affected data subjects if the breach will likely result in a high risk to their rights and freedoms.
- **Investigation:** Conduct a thorough investigation to determine the cause of the breach and implement corrective measures to prevent future incidents.

**Third-Party Data Processors.** The Company will ensure that any third-party service providers or contractors that process personal data on behalf of the Company adhere to the same data protection standards as set out in this Policy.

**Training and Awareness.** The Company will provide regular data protection training to all employees, ensuring they understand their responsibilities under this policy and relevant data protection laws. New employees will receive data protection training as part of their onboarding process.

**Compliance and Monitoring.** The Data Protection Officer (DPO) or other designated person oversees compliance with this Policy and relevant data protection laws.

Regular audits and assessments will be conducted to monitor compliance and identify areas for improvement.

Non-compliance with this Policy may result in disciplinary action, including termination of employment.

**PROTECTION OF YOUR PERSONAL INFORMATION.** We establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal information. We have in place the appropriate measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information stored on our Site.

To safeguard the confidentiality of personal information that we collect, we implement password protection and a variety of security measures to maintain the safety of your personal information

when you enter, submit or access your personal information. We use a secure server to protect your personal information and to prevent unauthorized access and disclosure.

Our security measures are regularly updated.

**Review and Amendment.** This Policy will be reviewed and updated as necessary to reflect changes in relevant data protection laws, Company's operations, or best practices.