DATA PROTECTION AND CONFIDENTIALITY STATEMENT

kasko2go AG, ref. # 1043-228-09, Blegistrasse 9, 6340 Baar, Switzerland, hereinafter referred to as the **"Processor"**, provides services to its **"Clients"** in conformance with this Data Protection and Confidentiality **"Statement"**.

Whereas:

1.1. The Client and the Processor have concluded a contract, hereinafter referred to as the **"Contract"**, pursuant to which the Processor provides services to the Client, hereinafter referred to as the **"Services"** or **"Service"**, that may entail the Processing of Personal Data as defined in Clause 1 of this Statement;

1.2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, hereinafter referred to as the GDPR, imposes specific obligation on the Client (the Controller as defined in Article 4 of the GDPR) with regard to the Client's partnerships. The GDPR requires the Client to conduct appropriate due diligence on the Processor and to have contracts containing specific provisions relating to data protection;

1.3. The Processor and the Client enter into a contract for processing by third parties within the meaning of Article 28(3) and Article 32 of the General Data Protection Regulation.

1.4. Kasko2go as an entity of Switzerland is also regulated by Datenschutzgesetz Schweiz 2023 – revDSG.

1.5. Specific regulations regarding Israeli data security will be described in the "Addendum" of this Statement.

2. DEFINITIONS

2.1. Terms and structure are aligned with ISO27001 and ISO27002 standards, 2022 versions.

2.2. For the purposes of this Statement, words and phrases in the Statement to the greatest extent possible shall have the meanings given to them in the GDPR, revDSG or ISO27001/ISO27002 standards. In addition to other terms defined herein, the following terms are used in this Statement:

2.2.1. Data Subject – identified or identifiable natural person who can be identified, directly or indirectly, and whose Personal Data is or may be processed as part of the provision of the Service;

2.2.2. Personal Data – any information relating to the identified or identifiable Data Subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2.2.3. Breach – any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

2.2.4. Processing – operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

2.2.5. Sub-processor – natural or legal person, public authority, agency or other body which is engaged in the Processing by the Processor and which following Processor's instructions processes Personal Data on behalf of the Client (including any affiliate of the Processor).

3. INFORMATION REGARDING PROCESSING

3.1.1. For the purpose of providing the Service, the Processor shall Process the Personal Data of the following Data Subjects:

3.1.2. Policyholder;

3.1.3. Insured.

3.2. For the purpose of providing the Service, the Processor shall Process the following Personal Data:

3.2.1. Address of Policyholder;

3.2.2. Address of the Insured.

4. OBLIGATIONS OF THE PROECSSOR

4.1. The Processor has an obligation to:

4.1.1. process the Personal Data only

a) if the Processing is necessary to provide the Services;

b) in accordance with the specific documented instructions of the Client;

c) if the Processing is necessary to comply with the applicable law (in which case, the Processor must provide prior notice to the Client of such legal obligation, unless the applicable law prohibits such disclosure;

d) in the amount necessary to provide the Services.

4.1.2. ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

4.1.3. take all security measures required by GDPR Article 32:

a) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, the Processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk;

b) in assessing the appropriate level of security to take into account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed;

c) to ensure that any person acting under the authority of the Processor who has access to Personal Data does not process them except on instructions from the Client, unless this person is required to do so by the applicable law;

d) taking into account the nature of the Processing, to reasonably assist the Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests for exercising the data subject's rights;

4.1.4. comply with and to reasonably assist the Client to comply with the obligations regarding the Breaches (as set forth in Articles 33 and 34 of the GDPR), data protection impact assessments (as set forth in Article 35 of the GDPR), and prior consultation (as set forth in Article 36 of the GDPR);

4.1.5. in accordance with the Client's instructions to delete all Personal Data or return it to the Client after the end of the provision of Services relating to Processing, and delete existing copies unless applicable law requires storage of the Personal Data;

4.1.6. provide the Client with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client.

4.2. The Processor must maintain all records required by Article 30(2) of the GDPR in writing, including electronic form, and the Processor must make them available to the Client upon Client's request to the extent they are applicable to the Processor's activities for the Client. The data shall be maintained in the terms stipulated in the applicable law.

4.3. In accordance with Article 28(1) of the GDPR, the Processor has implemented the following technical and organisational measures in such manner that

Processing of Personal Data by the Processor meets the requirements of the control and ensures the protection of the rights of the data subjects:

4.3.1. Secure network endpoints with vulnerability scanning;
4.3.2. Data loss prevention internal procedures;
4.3.3. Antivirus and firewall solutions;
4.3.4. CI/CD process contains a security scanning and reporting step to control dependencies and containers;
4.3.5. Google Workspace Directory (GWD) to control access to projects and Google Cloud Platform (GCP) Identity and Access Management (IAM) roles to separate access to GCP services in projects;
4.3.6. GCP (IAM) and GWD to control access to projects and GCP IAM roles to separate access to GCP services in projects;
4.3.7. Regular updates and patches;
4.3.8. Vulnerability management;
4.3.9. Internal procedures for managing and ensuring information security.
4.3.10. The pseudonymization and encryption of personal data;
4.3.11. The ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;
4.3.12. The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;
4.3.13. A procedure for regularly checking, evaluating and evaluating the effectiveness of technical and organizational measures to ensure the security of processing.

4.4. The Processor will implement, maintain and, if necessary, adapt the aforementioned measures in order to protect personal data from accidental or unlawful destruction, loss, falsification, unauthorized disclosure or access or other unlawful forms of processing. The aforementioned measures are also aimed at preventing unnecessary collection and further processing of personal data.

4.5. The Processor processes personal data only in the member states of the

European Union, the states of the European Economic Area or in any other European country, provided that this country is included in the list of third countries approved by the European Commission. Notwithstanding the provisions of this section, the Processor is permitted to process personal data on servers located in Israel. The Client consents to such processing, provided that the Processor ensures that such processing is carried out in accordance with applicable data protection laws, in particular the General Data Protection Regulation (GDPR), and the transfer of personal data to third countries. The Processor takes all necessary measures to ensure that such transfers of personal data to Israel are made in accordance with applicable data protection laws.

4.6. The Processor will instruct its employees or contract employees in such a way that they do not violate this order processing contract.

4.7. The Client and the Processor will inform each other about the upcoming changes in laws and regulations and will make desired or necessary adjustments by mutual agreement, e.g. in the processing process, safety measures and instructions and training for employees.

5. EXAMINATIONS

5.1. During office hours, the Processor shall grant the Client and the appointed auditors access to its premises and computerised systems in which personal data is stored and shall provide all information on the storage, processing and use of personal data that enables the Client and its auditors to verify whether the Processor is complying with its legal obligations under this Statement. The Processor will participate and provide all relevant information for the audit in good time.

5.2. The Processor may, with the consent of the Client, replace the audit with a third-party communication (TPM).

5.3. The persons who carry out an audit comply with the security procedures in force at the Processor, provided that these security procedures have been brought to the attention of the Client and sign a confidentiality agreement with the Client drawn up by the Processor before any activity.

5.4. The costs of an audit will be borne by the Client, unless the audit shows that the Processor has materially breached this Statement.

6. DELETION OF DATA

6.1. In accordance with Control 8.10/ISO27002 – Information deletion, and in accordance with Client's instructions to delete all Personal Data or return it to the Client after the end of the provision of Services relating to Processing, the Processor complies with the regulation and will delete existing copies unless applicable law requires storage of the Personal Data.

6.2. Sensitive information will be deleted when no longer required, by:

6.2.1. configuring systems to securely destroy information when no longer required

6.2.2. deleting obsolete versions, copies and temporary files wherever they are located using approved, secure deletion software to permanently delete information to help ensure information cannot be recovered by using specialist recovery or forensic tools;

6.2.3. using approved, certified providers of secure disposal services;

6.2.4. using disposal mechanisms appropriate for the type of storage media being disposed of (e.g. degaussing hard disk drives and other magnetic storage media)

7. TRANSFER OF INFORMATION BETWEEN PARTIES

7.1. Sensitive information will be transferred from the Client to the Processor through secure connection.

7.2. The Processor will manage a business continuity plan that will ensure, inter alia, the survivability and backup of the information systems that support the essential processes of all the subjects of this Statement.

8. ENGAGING OF SUB-PROCESSORS

8.1. The Processor must inform the Client of any intended changes concerning the addition or replacement of Sub-processors. The Client is entitled to object to such changes.

8.2. When engaging the Sub-processor, the Processor must impose the data protection obligations set forth in the Statement upon the Sub-processor, so that the Processor’s contract with the Sub-processor contains sufficient guarantees that the Processing will meet the requirements of the GDPR. The Processor is fully responsible for the performance of the Sub-processor's obligations and the Processing carried out.

8.3. The use of third parties is not to be understood as hiring additional capacities as employees of Processor. In the event that the Processor hires additional capacity, the Processor will set the same conditions that it requires of its employees.

9. INCIDENTS

9.1. The Processor must notify the Client immediately without any undue delay but not later than 72 hours in the event of any Personal Data Breach or any suspicions on Personal Data Breach. The notification shall contain at least the following information:

9.1.1. The nature and extent of the data breach, including, but not limited to, the time of the data breach, the time of notification/discovery, the number of data subjects, the content and nature of the incident, the verified and likely consequences);

9.1.2. Recommended measures to limit the negative consequences of the data breach;

9.1.3. Measures implemented or proposed by the Processor to remedy the consequences.

10. RECRUITMENT

10.1. In accordance with ISO27002 standard Controls 6 – People controls, the following measures will be applied:

10.1.1. For positions defined as sensitive by the Processor (such as those that allow access to sensitive information or have permissions that could endanger the company), controls are in place to assure the candidates' suitability.

10.1.2. A contract signed with new employees, including a contract with manpower/placement companies, will include reference to the employee's responsibility in all aspects of cyber risks.

10.1.3. The Processor's employees who change positions or terminate their employment will be blocked from accessing information they do not need to perform their duties.

10.1.4. The Processor will conduct periodic training for employees in order to raise awareness of information security and cyber risks, according to the type of job performed.

11. LIABILITY

11.1. The Processor is fully materially liable for any damages caused to the Client or the Data Subject by violation of the requirements in the Statement or the GDPR or the Client's instructions.

12. OTHER PROVISIONS

12.1. In case of discrepancies between the conditions defined in the Statement and the Contract, the conditions set in the Statement shall prevail. In case of discrepancies between the conditions defined in the Statement and applicable laws (e.g. GDPR or revDSG), the laws shall prevail.

12.2. Any amendments and addendums/supplements to the Statement are in effect only if made in written and signed by duly authorized representatives of the Parties.