PRIVACY POLICY FOR PARKIZA PLATFORM ("**Policy**")

1. **General information**
   1.1. Signal OS Tech sp. z o.o. (ul. Rondo Ignacego Daszyńskiego 1, 00-843 Warsaw), entered in the register of Entrepreneurs of the National Court Register kept by the District Court for the Capital City of Warsaw in Warsaw, 13th Commercial Department of the National Court Register under KRS No.: 0000926854, REGON No.: 520194310, NIP No.: 5272974115 ("**Company**") provides services of managing specific functions of parking lots located in or at selected buildings ("**Services**") – basic functionalities of the Services are available at https://www.parkiza.com/.
   1.2. The platform providing the Services is available through the website or the mobile version of the platform made available on Google Play and App Store as a mobile application ("**Signal OS**").
   1.3. You can contact the Company at the e-mail address: contact@signalos.io, by phone at +48 519 441 304, or in writing to the address indicated above.
   1.4. The Company has appointed a Data Protection Officer. The Data Protection Officer can be contacted as specified in section 1.3 of the Policy.
2. **Information on the processing of personal data**
   2.1. The Company, in providing the Services through Signal OS, **is the controller of the personal data** ("**Data**") **of the following entities** ("**Data Subjects**"):
      a) owners/tenants of parking spaces in parking lots located in or adjacent to buildings for which Services are provided through Signal OS ("**Customers**"), and with whom the Company has entered into a contract for the provision of services ("**Contract**") – if the Customer is a natural person who has downloaded Signal OS and created a user account with Signal OS;
      b) natural persons representing Customers; and
      c) natural persons designated by the Customer to contact the Company to perform the Services.
   2.2. The Company received the data of the Data Subjects indicated in sections 2(2.1.)(b) and (c) of the Policy, from the Customer whose representatives are Data Subjects or on whose behalf Data Subjects act.
   2.3. In the course of providing the Services through Signal OS, the Company **is not a controller of the data** of employees/associates of Customers who have downloaded Signal OS and created a user account in Signal OS ("**Users**") and guests of Customers ("**Guests**") to whom the Customer temporarily provides parking spaces. The Data is entrusted to the Company by the Customer under the terms and conditions referred to in sections 3-6 of the Policy.
   2.4. The Company may process Data Subjects' Data:
      a) **in order to perform a contract for the provision of Services** (Article 6(1)(b) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)("**GDPR**");
      b) **in order to comply with the Company's legal obligations** (Article 6(1)(c) of the GDPR), e.g. under tax legislation;
      c) **in order to exchange correspondence** (Article 6(1)(f) of the GDPR) based on the Company's legitimate interest in contacting Data Subjects through communications sent via Signal OS, electronic mail (e-mail), traditional mail, telephone, as well as via the contact form on the website;
      d) **in order to establish, assert, or defend itself against claims** (Article 6(1)(f) of the GDPR), based on the Company's legitimate interest, such as responding to claims of Data Subjects.
   2.5. The scope of Data processed shall include at least (common data): name and surname/company, email address, the operating system of the device used ("**Device**"), system version of the Device, device ID of the Device, name of the network/mobile operator of the Device, IP address, telephone number, and position/function performed.
   2.6. The Company shall process the Data of: (a) Customers – for the period of their use of the Services; (b) Data Subjects (other than Customers) – until we receive a request to delete the Data from the Data Subject,
   unless the processing of the Data is necessary to comply with a legal obligation under applicable laws or to establish, assert or defend the Company against claims. The period of Data processing may be longer if applicable laws (national or EU) impose such an obligation on the Company.
   2.7. Data may be **shared with**: (a) entities authorized by law (e.g. courts); (b) subcontractors and other

entities providing services to the Company, including, in particular, entities providing accounting, IT, marketing, communication and analytical, legal and debt collection services; (c) in the case of Customer Data – to owners or managers of buildings or parking lots where the Services are provided.

2.8. The Data Subject has the right to:

a) request access to the Data and receive copies of the Data;
b) rectification (correction) of the Data;
c) deletion of the Data – if there is no legal basis for the Data to be processed;
d) restriction of Data processing – if the Data processed by the Company is incorrect or processed unreasonably, or if deletion is impossible due to the existence of a valid legal basis for processing;
e) portability of Data – the right to receive the Data in a structured, commonly used machine-readable format; including the right to send the Data directly to another entity;
f) object to the Company's processing of the Data – in the case of processing to pursue a legitimate interest;
g) lodge a complaint to the competent supervisory authority (President of the Personal Data Protection Office – ul. Stawki 2, 00-193 Warsaw).

In order to exercise the aforementioned rights, you should contact the Company using the contact details provided in section 1(1.3) of the Policy.

2.9. **Provision of Data is voluntary** but necessary for the Company to properly perform the Services and implement the objectives indicated in section 2(2.4) of the Policy. A refusal to provide the Data may result in the inability to use all Signal OS functions.

2.10. The Company may transfer Data outside the European Economic Area ("**EEA**") – the transfer will take place based on appropriate legal mechanisms, such as standard contractual clauses or other similar legal instruments provided for in the GDPR.

3. Scope of entrusted personal data

3.1. In order to enable the provision of the Services, the Customer entrusts the Company with the processing of the personal data specified in sections 3(3.2.) and (3.3.) of the Policy ("**DPA**"), under the terms and conditions specified in sections 3-6 of the Policy.

3.2. The Customer entrusts the Company with personal data regarding the User or Guest (ordinary data) such as email address, the operating system of the Device, system version of the Device, device ID, and network/mobile operator's name – as their controller or as a processor. The entrusted data are transferred as part of the use of the Services.

3.3. The Customer may also entrust additional personal data of the User or Guest: name, surname, vehicle registration number, IP address and telephone number.

3.4. The data entrusted to the Company indicated in sections 3(3.2.) and (3.3.) of the Policy ("**Entrusted Data**") shall not be subject to automated decision-making, including profiling.

4. Determination of the purpose, nature, and duration of the entrustment of the processing of Entrusted Data

4.1. The Entrusted Data shall be entrusted at the request of the Customer and solely for the performance of the Service by the Company. The conclusion of the DPA constitutes the above-mentioned documented request.

4.2. The Entrusted Data shall be processed by the Company on a permanent or occasional basis, depending on the specific activities performed in the performance of the Service.

4.3. Within 30 (thirty) days from the date of termination of the DPA or receipt of a written request for deletion of the Entrusted Data from the Customer, the Company shall, at the Customer's discretion, delete or return all Entrusted Data, from all media, programs and applications, including copies, unless the obligation to further process them arises from the law. This period is due to the necessity to create data backups to maintain data integrity during the provision of the Service.

4.4. The DPA shall terminate upon termination of the Contract.

5. Rights and obligations related to the processing of Entrusted Data

5.1. The Customer shall ensure that the Entrusted Data entrusted to the Company (including the Entrusted data entered into Signal OS directly by the Users) are processed by it on one of the relevant legal grounds outlined in Article 6(1) of the GDPR; or the Customer shall be entitled to entrust the Entrusted Data to the Company for processing.

5.2. Any person authorized by the Company to process Entrusted Data shall be required to maintain the confidentiality of such data.

5.3. The Company undertakes to apply technical and organizational measures adequate to the identified risk of violation of the rights or freedoms of the User or Guest.

5.4. The Company undertakes to cooperate with the Customer in responding to User or Guest requests as described in Chapter III of the GDPR.

5.5. The Company undertakes to assist the Customer in complying with the obligations outlined in Articles 32-36 of the GDPR, in particular in reporting breaches of protection of Entrusted Data to the supervisory authority, notifying the User or Guest of a breach of the protection of Entrusted Data.

5.6. The Company shall provide the Customer with all information necessary to demonstrate compliance with the obligations outlined in Article 28 of the GDPR, and allow the Customer or an authorized auditor to conduct audits. The Company undertakes to immediately inform the Customer if, in its opinion, the instruction given to the Customer constitutes a violation of the provisions of the GDPR or other EU or Member State data protection legislation.

5.7. The right to conduct the aforementioned audits may be exercised during the Company's business hours, i.e. from Monday to Friday from 9.00 am to 5.00 pm excluding public holidays and with a minimum of seven days' notice, and shall not interfere with the Company's operations. The Customer shall bear all costs associated with the aforementioned audits on its own. If any deficiencies are found during the audit, the Company undertakes to rectify them within the time-limit agreed with the Customer.

5.8. The Company undertakes, upon discovery of a breach of protection of Entrusted Data, to promptly notify the Customer of this. The information provided to the Customer shall include, at a minimum: a description of the nature of the breach and, if possible, an indication of the category and an approximate number of persons whose data has been breached, as well as the amount/type of data affected by the breach; a description of the possible consequences of the breach; a description of the measures applied or proposed to be applied to remedy the breach, including the minimization of its negative effects.

6. **Use of Subprocessors**

6.1. In order to properly provide the Services, the Company shall use the services of third-party entities providing services to the Company ("**Subprocessors**"). The Customer gives its general consent for the Company to use the services of such entities and to further entrust them with the processing of the data entrusted to the Company.

6.2. The Company agrees to impose on the Subprocessors the same obligations to protect the Entrusted Data as outlined in the DPA.

6.3. The Company undertakes to inform the Customer of any intended changes regarding the addition or replacement of Subprocessors, thereby giving the Customer the opportunity to object to such changes ("**Objection**").

6.4. The Customer shall make an Objection in writing under pain of nullity within 7 (seven) days from the date of receipt of the information on the aforementioned changes, and shall provide adequate justification. A failure to make an Objection within the aforementioned time-limit shall be tantamount to consent to the change. The Customer agrees not to make an Objection to the above-mentioned changes without valid reasons.

6.5. If the Customer makes an Objection, it may be impossible to provide the Services. In such a situation, the Company will be entitled to terminate the Contract and the DPA without notice. In such a situation, the Company shall not be liable for the termination of the aforementioned Contract and Agreement.

6.6. The Company shall be entitled to further entrust the processing of Entrusted Data to entities outside the EEA. If the Company is required to transfer Entrusted Data outside the EEA under generally applicable laws, the Company shall inform the Customer prior to the transfer of such data of that legal obligation, unless the Company is prohibited by law from providing such information due to an important public interest.

6.7. The Company may transfer Entrusted Data outside of the EEA only if it complies with the specific requirements outlined in Chapter V of the GDPR "Transfer of Entrusted data to Third Countries or International Organizations" and, in particular, ensures that the transfer of Entrusted Data takes place based on the relevant legal mechanisms, in particular, the European Commission's implementing decisions, standard contractual clauses or other similar legal instruments provided for in the GDPR.

7. **Final Information**

The development of technology and the development of the Company's offerings mean that the Policy may change. The Company will provide information about the change of the Policy through Signal OS.