DATA PROTECTION AND DATA MANAGEMENT INFORMATION
PS Sol-PC Ker Kft Ltd.

effective on: July 1, 2020

The company PS Sol - PC Ker Ltd. (head office: Hu-1063 Budapest, Szinyei Merse utca 10, business registration number: 03-09-126056, tax number: 24136231-2-42, representative: Miklós Szabados, e-mail: pskerkft@gmail.com, telephone: +36 70 362-1047, hereinafter referred to as 'the company', provides the following information on its data management activities in accordance with Regulation No 2016/679 of the European Parliament and of the Council on the General Data Protection (hereinafter referred to as 'GDPR').

1. Our data management activities:

The company acts as data controller with respect to personal data relating to the following activities:
• receipt of call for offers from our customers, offering, contracting,
• maintaining relationships with our customers ,
• establishment and maintenance of employment relationships, recruitment.

2. Scope of personal data managed by the company:

In the course of the data management, our company handles the names, addresses, mother's names, places and data of birth, identity card numbers, phone numbers, e-mail addresses of natural persons (in the event of its employees - social insurance numbers, tax numbers, driving license numbers), and in the event of non-natural persons - the company handles the names of contact persons, their phone numbers and e-mail addresses.

3. Purpose of the company's data management activities:

The company handles the named personal data for the following purposes:
• to conclude, perform and fulfil the contracts, which are necessary for performance of the company's data management activities, or for the claims or law enforcement resulting from the concluded contracts, for communication and contacts, for billing,
• to send letters with regular information related to your business,
• to record our partners' data for business and marketing strategy, or for other business events,
• to keep statutory records and registration of our employees, to prepare declarations and reports, to perform rights and obligations arising from employment,
• to recruitment or to select our prospective employees,
• to enforce our legitimate interests as a data controller.
The company may process personal information in order to achieve any of the data management purposes described above.
The company does not use the given personal information for the purposes other than those described in these points.

4. Legal basis of the company's data management activities:

• contribution of the person concerned: in accordance with point (a) of Article 6 (1) of the GDP Regulation, the user's voluntary contribution to data management based on appropriate information;
• performance of the contract: in accordance with point (b) of Article 6 (1) of the GDP Regulation, the data management is required to fulfill the contract, in which the parties concerned is a contracting party;
• compliance with legal obligations: data management is required to comply with the legal obligation of the data controller (such as accountancy and bookkeeping, data reporting obligations in compliance with labour law) pursuant to point (c) of Article 6 (1) of the GDP Regulation;
• legitimate interest: GDP 6. in accordance with point (f) of Article 6 (1) of the GDP Regulation, data management is

necessary to ensure the legitimate interests of the data controller or of a third party.

5. Information on the data managing person:

During the performance of hiring employees and payroll accounting duties, the personal data managed by the company shall be handled by Mrs. Tokodiné Erzsébet e.v. as an accountant of the company, as well as during the performance of the tasks related to invoicing matters, the personal data managed by the company shall be handled by Mrs. Tokodiné Erzsébet e.v. as an accountant of the company, together with FEIGL AUDIT Ltd. as an auditor of the company, treated here as a data processor. NETCLASS Ltd carries out the company's IT operational activities as a data processor

The transmission of data to the data processor may be carried out without an explicit consent of the affected data subject. The disclosure of personal data to third parties or to official authorities may be made only on the basis of an official decision or subject to the prior explicit consent of the subject of the affected data, unless otherwise provided by law.

6. Data transmission:

In compliance with the statutory obligation of the company, the Company shall forward the buyer's and seller's information, the invoiced items, and specified details of the invoice to the Hungarian National Tax and Customs Office (NAV).

The company shall not forward any personal data to a third country that is not a party to the GDP regulation, within the meaning of GDP regulation, and the named personal data are only transmitted to the data processor named in this prospectus, and exclusively for the designated purpose.

7. Principles of data management at the Company (hereinafter referred to as Data controller):

Data controller handles the personal information in accordance with the principles of good faith, upright and transparency, in accordance with existing legislation and with the provisions of this information leaflet.

The data controller shall use the personal data strictly in accordance with necessity for the performance of the services provided by the data controller on the basis of the consent of the subject of the affected data and solely for designated purposes.

The data controller shall handle personal data only for the purpose specified in this prospectus and in the relevant legislation. The scope of the personal data handled is proportionate to the purpose of the data processing and should not extend beyond it.

The data controller may not handle personal data of a person under the age of 18.

Data controller does not verify the personal data provided. Only the person giving the personal data shall be responsible for the adequacy of the personal data provided.

The data controller shall not transfer any personal data processed by him to any third party other than the data processor specified in this prospectus or to the public bodies specified to fulfil the statutory reporting obligation.

In certain cases, for example, for legal proceedings due to the copyright, property and other kind of infringement. or because of their thorough suspicion of the affected data subject, prejudice to the interests of the data controller, endangering the provision of services, etc., at the request of an official court, police, the data controller may makes available a certain personal information of the subject of the affected data available to third parties.

The data controller shall ensure the security of personal data provided, the data controller shall take the technical and

organisational measures and shall establish rules of safe procedure to ensure that the data collected, stored or handled are protected or prevented from being accidentally lost, unlawfully destroyed, unauthorised accessed, unauthorised used and unauthorised changed or disseminated. To fulfil this obligation, the data controller shall call and engage any third party to whom he transmits the affected personal data.

In view of the relevant provisions of GDP regulation, the data controller is not required to appoint a data protection officer.

8. Access to personal data on the part of the Company employees:

The company provides its employees with access only to the personal data they manage in order to provide the service that is strictly necessary for their work. All kinds of access shall be logged, and only the IT systems' operator has access to the data extraction function.

The data controller is performing the data back-up operations by encryption through the data processor, thus in case of data recovery it renders possible that the employees will not have access to the saved personal data. Employees of the company do not have access to servers with live or sensitive data.

9. Data subject's rights to the processing of his / her personal data:

9.1. <u>Right of access:</u>

The subject of the affected data may request the company to inform him / her whether the company is managing the personal data of subject of the affected data and, if so, to provide him / her with access to the personal data that company manages. The subject of the affected data may request information by e-mail to his/her e-mail address at any time, in writing, by registered or registered letter to the address of the company, or by e-mail: pskerkft@gmail.com. The request for information sent in the letter shall be considered credible if, on the basis of the request sent, the person concerned can be clearly and unambiguously identified. A request for information sent by e-mail shall be considered credible only if it is sent by the subject of the affected data from the e-mail address provided by him/her to the company, but this does not preclude the company from identifying the subject of the affected data in another way before the requested information will be provided.

The request for information may include the data of the subject of the affected data managed by the company, their source, the purpose of use, legal basis of processing, duration, the name and address of any data processor, the activities related to the processing of data.

9.2. <u>Right to rectification:</u>

The subject of the affected data may request the correction, clarification or modification of personal data managed by the company. Taking into account the purpose of data processing, the subject of the affected data may request a complementation of incomplete personal data. Once the request for the modification of personal data has been made, the previous (deleted) data cannot be recovered.

9.3. <u>Right to cancellation:</u>

The subject of the affected data may request the deletion of personal data processed by the company. Cancellation may be refused

- to exercise the right to freedom of expression and information, or
- if the processing of the personal data is authorised by law; and
- to submit, enforce or protect legal claims.

In all cases, the Company shall inform the subject of the affected data about the refusal of the deletion request,

indicating the reason for refusing to deletion. Once the request for the deletion of personal data has been fulfilled, the previous (deleted) data cannot be recovered.

9.4. Right to restriction of data processing:

The subject of the affected data may request the data controller to restrict the processing of his/her personal data, if the subject of the affected data disputes the correctness of the personal data processed. In this case, the restriction applies for the period of time allowed for the company to verify the correctness of the personal data. The Company shall indicate the personal data it manages if the subject of the affected data disputes its correctness or accuracy, but the correctness or inaccuracy of the contested personal data cannot be clearly established. Furthermore, the subject of the affected data also may request the data controller to restrict the processing of his/her personal data, if the purpose of data management is implemented, but the subject of the affected data requests the processing of the data by the data controller for the submission, validation or protection of his/her legal claims.

9.5. Right to protest:

The subject of the affected data may object to the processing of his / her personal data,
• if the processing of personal data serves for the sole purpose of fulfilling the legal obligation of the data controller, or necessary for the legitimate interest of the data controller or third party;
• where the personal data are processed for the purposes of direct marketing, public opinion polling or scientific research; or
• when the personal data are processed in order to fulfil a public interest task.

The data controller shall examine the lawfulness of the objection of the subject of the affected data and, where there is justified opposition, shall terminate the processing of the data and block the personal data processed and shall notify all the measures taken on the basis of the objection to all the persons to whom the personal information of the subject of the affected data has been previously transmitted.

9.6. Right to withdraw consent:

The subject of the affected data shall at any time have the right to withdraw his / her consent to the processing of personal data processed previously with his / her consent. The withdrawal shall be without prejudice to the lawfulness of data processing prior to the withdrawal of the consent. You can withdraw your consent by sending your letter with withdrawal by e-mail to the e-mail address pskerkft@gmail.com.

9.7. Right to data portability:

The subject of the affected data may request the data controller that the personal data provided by him/her shall be provided or forwarded either on paper, or in a widely used, structured machine – readable format (XML / XLS / CSV) to another data controller.

10. Security of data:

The following security measures to processing information have been introduced and applied by the company to protect your data:

10.1. Physical security

The head office of the company has an electronic access control system and a concierge service too. The company has a camera system at its headquarters and premises, providing security against unauthorised or forced entry, fire or natural disaster. Personal data handled on a paper basis is stored in a closed location, which can only be accessed by a limited personal with access rights.

10.2. Data security in IT infrastructure

Personal data is stored on servers provided by the hosting provider, which can only be accessed by a very limited personal and employee group under strict privacy policy. IT systems are re-tested and monitored regularly to ensure and maintain data and IT security. Office workstations are password protected, use of foreign media is regulated and allowed only under safe conditions, after verification. Systematic and continuous protection against harmful software covering all our systems and elements of the systems is provided. The design, development, testing and operation of programmes, applications and tools shall be conducted with priority and isolation of security functions.

10.3. Data security in communication

We ensure the integrity of processing data both for (Communication) Control and for user data in order to meet the requirement of secure data exchange for electronically transmitted messages and files. Procedures for error detection and correction are used to prevent data loss and injury. With regard to applications, passwords, privileges and other security-related parameters, data may be transmitted only if they are encrypted. We prevent data loss and damage by using fault detection and correcting procedures and secure that principles of non-denial are ensured. In the case of the network used for data transmission, we provide the security level in accordance with the prevention of illegal connection and eavesdropping.

10.4. Data security during the document management

We also comply with the requirements of data security, which are set out in the record management regulations. Document management shall be carried out according to written authorization levels according to the security standards applied to the confidentiality of each document. We have detailed and strict rules on the destruction (shredding), storage and publication of documents.

11. Measures in the event of a Data Protection incident

Any incidents with data protection that may arise will be reported to the Supervisory Authority in accordance with the law within 72 hours of becoming aware of this Data Protection incident, and we will also keep a record of all data protection incidents. In the cases provided for by law, the subjects of the affected data will also be informed of the occurred incident.

12. Duration of Data Processing

The data contained in the contract concluded with the customers shall be retained for a period of five years after the performance of the contract.

In order to comply with the requirements of accounting and tax legislation, personal data shall be kept for seven years following the end of the tax year.

The employment records shall be kept for a period of 4 years after the termination of the employment relationship.
The personal data provided during the subscription to the Newsletter will be retained for 3 years.

13. Opportunities to enforce the rights

You can contact our company with any questions or comments regarding the data management:
e-mail: pskerkft@gmail.com
telephone: +36 70 362-1047

The subject of the affected data can refer his/her complaints concerning the management of his/her data by the company directly to the Nemzeti Adatvédelmi és Információszabadság Hatóság, which is the National Authority of Data Protection and Freedom of Information. (address: Hu-1125 Budapest, Erzsébet fasor Szilágyi 22/C; telephone: + 36-1-391-1400; e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu).

In the event of a breach of the rights concerned the aggrieved subject of the affected data can appeal to the court. The Törvényszék (General Court) shall have jurisdiction to hear and determine actions or proceedings. At option of the subject of the affected data, proceedings in respect of the claim may be brought in the court of the place of residence or stay of the person concerned. Upon request, the data controller shall inform the user about the possibility and tools of the remedy.

14. Terms used in the prospectus:

14.1. '***personal data***' means any information relating to an identified or identifiable natural person ('***data subject***'); a natural person who can be identified, directly or indirectly, in particular by means of an identifier such as name, number, location data, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person may be identified;

14.2. '***data processing'*** means any operation or set of operations carried out on personal data or files, whether automated or non-automated, such as collection, recording, organisation, layout, storage, transformation or alteration, consultation, examination, use, disclosure, transmission, dissemination or otherwise making available, alignment or interconnection, restriction, erasure or destruction;

14.3. '***data controller***' means any natural or legal person, public authority body, agency or any other body which defines the purposes and means of processing personal data individually or in conjunction with others; where the purposes and means of processing are determined by Union or national law, the data controller or specific criteria for the designation of the data controller may also be determined by Union or national law;

14.4. ***'data processor'*** means any natural or legal person, public authority body, agency or any other body, which manages personal data on behalf of the data controller;

14.5. '***consent of the person concerned***' means a clear and unambiguous, voluntary and concrete statement of the will of the person concerned (subject of the affected data), based on appropriate information, by which the declaration or the confirmation of the person indicates by means of an act which is unambiguous, that he/she has given consent to the processing of his/her personal data concerning his/her personality;

14.6. '***data protection incident***' means an injury to security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access of personal data transmitted, stored or otherwise processed.

Budapest, July 1, 2020

PS Sol - PC Ker Kft