PRIVACY POLICY

ROYAL SPED Szállítmányozói Zártkörűen Működő Részvénytársaság , acting as Data Controller, is fully committed to protect the privacy and personal information of clients and business partners, undertakes to operate in compliance with relevant privacy laws and ensure the secure and lawful handling of personal data. Pursuant to Article 13 and Article 14 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 personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as "General Data Protection Regulation" or "GDPR") the Company has prepared and implemented the following Privacy Policy:

I) INTRODUCTION

Information about Data Controller:

Company name: **ROYAL SPED Szállítmányozói Zártkörűen Működő Részvénytársaság**

Registered seat: H- 1239 Budapest, Európa utca 6, B1 épület

Company registration number: 01-10-043532

Website: www.royalsped.eu

Email: royal@royalsped.eu

Telephone: +36-1-421-8538

Data Controller shall always handle personal information received from Data Subjects in accordance with relevant Hungarian and EU privacy laws and ethical standards, and take all technical and organizational measures necessary for the secure handling and processing of personal data.

This Privacy Policy was prepared in consideration of the following laws and regulations:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as "GDPR");

- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter referred to as "Privacy Act").

Pursuant to relevant provisions of GDPR, Data Controller shall not designate a data protection officer.

II) DEFINITIONS

For the purposes of this Privacy Policy the following capitalized terms shall have the meaning set out below.

Data Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller;
Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Data Controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law, the Controller or the specific criteria for its nomination may be provided for by EU or Member State law;
Marking: means flagging certain personal data for a specific purpose;
Transfer: means sending or making available the personal data to a third party;
Erasure: means deleting the personal information in a way that makes recovery or restoration impossible;
Personal data breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
EEA country: means any of the member states of the European Union and member states of the agreement on the European Economic Area, and other non EEA member countries whose citizens have the same rights as those of EEA members states pursuant to an international agreement executed between the European Union and the non EEA member country.
Data Subject: means a natural person directly or indirectly identified or identifiable by reference to personal information;

Third country: means any country that is not an EEA country;

Third party: means a natural or legal person, or any association not having legal personality other than the data subject, Controlleror the processor

Consent: consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Binding corporate rules: means personal data protection policies approved by the National Authority for Data Protection and Freedom of Information (hereinafter referred to as “Authority” or “NAIH”) which are adhered to by a Controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a Controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

Data to be disclosed in the public interest: any data and information that is not regarded as “data of public interest” but whose disclosure is “in the public interest” and is mandated by law;

Special categories of personal data:

1. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or concerning a natural person's sexual orientation
2. data concerning health, addictions, criminal convictions or offences;

Disclosure: means making the information accessible by anyone;

Personal data: means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one 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.

Objection: means a written request by Data Subject asking Controller to stop processing his/her personal data and have the processed personal data deleted;

Data processing: means carrying out of technical exercises related to data management processes, regardless of the method and instruments applied for accomplishing these operations, as well as the place of accomplishment, given the technical exercise is carried out on the data;

Destruction: total physical destruction of the data carrier that holds the personal data;

Data of public interest: means any data or information other than personal data which is collected, controlled, stored or processed by governmental/public organizations and is related

to the operation of such organization, including but not limited to scope of responsibility, organizational structure, activities performed, evaluation of performance, executed contracts and agreements, type of information processed.

III) PRINCIPLES OF DATA PROCESSING

1) Lawfulness, fairness and transparency

Data Controller shall process personal data always in a lawful, fair and transparent manner in relation to data subjects.

2) Purpose limitation

Data Controller shall collect personal data only for specified, explicit and legitimate purposes and is not allowed to process them further in a way that is not compatible with those purposes.

3) Data minimization

Data Controller shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4) Accuracy

Data Controller shall ensure that personal data are accurate and are kept up to date where it is necessary. Personal data that are inaccurate – considering the purposes for their processing – must be deleted or rectified without any delay.

5) Storage limitation

Data Controller shall ensure that personal data is kept in a form that makes it possible to identify data subjects for no longer than is necessary for the purposes of the processing.

6) Integrity and confidentiality

Data Controller shall take appropriate technical or organizational measures to ensure appropriate security and protection of personal data.

IV) LEGAL BASES FOR PROCESSING

- Issue invoices in accordance with accounting laws and regulations

Legal basis: Article 6 (1) (c) of GDPR

Data retention period: 8 years from issue of invoice

- Contact and communication

  Legal basis: Article 6 (1) (f) of GDPR

  When processing personal data of employees of clients and business partners, evaluate whether interests are overridden by the interests or fundamental rights and freedoms of the data subject.

  Legitimate interests pursued by Controller: continuity of business.

  Data retention period: document/file retention period according to the subject of the agreement
- Process personal data of employees

  Legal basis: Article 6 (1) (b) (c) of GDPR

  Data retention period: document/file retention period according to the subject of the agreement
- Process personal data of clients and business partners

  Legal basis: Article 6 (1) (b) of GDPR

  Data retention period: document/file retention period according to the subject of the agreement
- Marketing

  Legal basis: Article 6 (1) (a) of GDPR
- Operate surveillance cameras

  Legal basis: Article 6 (1) (f) of GDPR

  Legitimate interests pursued by Controller: protection of company assets and legitimate interests of employer as set out in the Labour Code

Collection of personal data is based on freely given consent of the data subject. Where we need to collect personal data by law, or under the terms of a contract we have with the data subject and data subject fails to provide that data when requested, we may not be able to perform the contract or provide the agreed services, as listed below:

- if data collection is necessary for compliance with a legal obligation to which the Controller is subject: legal obligation can not be fulfilled
- if data collection is necessary for execution of contract: contract can not be executed
- if data collection is necessary for provision of services: services can not be provided
- if data collection is necessary for security reasons: limitation or denial of access

V) WHO HAS ACCESS TO COLLECTED PERSONAL DATA

Collected and stored personal data can be accessed only by Data Controller and employees of Data Controller.
Personal data may be transferred only if required by law and if Data Subject consents to the transfer.

VI) RIGHTS OF DATA SUBJECTS

1) Right of access

The data subject shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2) Right to rectification

The data subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3) Right to erasure

The data subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay and the Controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;

c) the data subject objects to the processing where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller or for the purposes of the legitimate interests pursued by the Controller or by a third party and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State (Hungarian) law to which the Controller is subject;

f) the personal data have been collected in relation to the offer of information society services.

4) Right to restriction of processing

The data subject shall have the right to obtain from the Controller restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the Controller to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d) the data subject has objected to processing pending the verification whether the legitimate grounds of the Controller override those of the data subject.

A data subject who has obtained restriction of processing shall be informed by the Controller before the restriction of processing is lifted.

5) Right to object

- The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller or for the purposes of the legitimate interests pursued by the Controller or by a third party, including profiling based on those provisions.

- The Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

- Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, the right to object shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

VII) PERSONAL DATA BREACH

1. Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed by Data Controller.

2. All Employees shall promptly notify their supervisor about any detected or suspected personal data breach. Data Controller, as employer, shall promptly investigate the reported data breach, and shall, within 2 working days of learning thereof, describe measures proposed to be taken to remedy the data breach to Employer’s managers in charge.

3. In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to supervisory authority NAIH, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. The notification to NAIH shall at least:
   - describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   - communicate the name and contact details of the data protection officer;
   - describe the likely consequences of the personal data breach;
   - describe the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where the investigation by Data Controller concludes that the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, Data Controller shall promptly notify Data Controller's executives in charge, the chief executive officer, the senior legal counsel of the company group, and the managers of the area where the data breach was detected. Employer shall notify all Data Subjects within 72 hours of detecting the data breach.
5. Employer shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. The documentation shall:
   - describe the personal data records concerned;
   - describe the categories and approximate number of data subjects concerned;
   - describe data and time of the data breach;
   - describe the circumstances and consequences of the data breach;
   - describe the measures taken or proposed to be taken to address the personal data breach.
6. The documentation shall be retained by Employer for 5 years from detecting the data breach.

VIII) SECURITY OF DATA PROCESSING

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with relevant laws and regulations. Such measures include but are not limited to:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Personal data provided by Data Subjects shall be stored by Data Controller at Data Controller's headquarters or registered business site.

IX) REMEDIES, COMPLAINTS

1) Right to lodge a complaint with a supervisory authority

Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Privacy Policy and/or any related law or regulation.

Complaints may be lodged with the following supervisory authority:

Hungarian National Authority for Data Protection and Freedom of Information

(Nemzeti Adatvédelmi és Információszabadság Hatóság ,NAIH)

Registered seat: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Postal address: 1530 Budapest, Pf.: 5

Email: ugyfelszolgalat@naih.hu

Telephone number: +36 (1) 391-1400 Fax.: +36 (1) 391-1410

Website: www.naih.hu

2) Right to an effective judicial remedy against a supervisory authority

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person data subject shall have the right to an effective judicial remedy:

 against a legally binding decision of a supervisory authority concerning them;

 where the supervisory authority does not handle a complaint;

 where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint

 where the Data Subject considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR.

3) Right to send inquiries, suggestions

Every data subject shall have the right to contact the employees of Data Controller at **royal@royalsped.eu** with any inquiry, suggestion or question related to the processing of personal data.

X) MISCELLANEOUS

1) Data Controller undertakes to ensure the security and confidentiality of collected and processed personal information and to take all necessary technical measures to guarantee the protection of collected/stored/process personal data from unauthorized use, access, modification, disclosure, destruction or erasure. Data Controller also undertakes to ensure that any third party, to whom personal information is transferred, is also obligated to ensure the same level of data protection.

2) Data Controller reserves the right to amend or modify this Privacy Policy with prior written notice sent to data subjects. The continued use of services by Data Subjects shall be regarded as acceptance of the modified Privacy Policy.

This Policy is effective as of 25 May 2018