DATA PRIVACY POLICY

PEKO Spedycja Międzynarodowa | PEKO International Forwarding

PEKO Spedycja Międzynarodowa W. Jankowski, P. Stachura, Spółka Jawna
Miałki Szlak 4/8, 80-717 Gdańsk, KRS: 0000579319, NIP: 5832962551

TABLE OF CONTENTS:

1. Glossary of terms.

For the purposes of this documentation, the terms indicated shall have the following meanings:

1) **„personal data”** means information about 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person;

2) **„processing”** means an operation or set of operations performed on personal data or sets of personal data in an automated or non-automated manner, such as collection, recording, organizing, structuring, storing, adapting or modifying, retrieving, viewing, using, disclosing by transmission, dissemination or otherwise making available, matching or linking, limiting, erasing or destroying;

3) **„limitation of processing”** means marking stored personal data to limit future processing;

4) **„profiling”** means any form of automated processing of personal data that involves the use of personal data to evaluate certain personal factors of an individual, in particular to analyze or forecast aspects of that individual's performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movement;

5) **„pseudonymization”** means the processing of personal data in such a way that they can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and is covered by technical and organizational measures that prevent its attribution to an identified or identifiable natural person;

6) **„dataset”** means a structured set of personal data available according to specific criteria, regardless of whether the set is centralized, decentralized or functionally or geographically dispersed;

7) **„admin”** means a natural or legal person, public authority, entity or other body that 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 Union or Member

State law, a controller may also be designated by Union or Member State law, or specific criteria for its designation may be set forth;

8) **„processor”** means a natural or legal person, public authority, entity or other entity that processes personal data on behalf of the controller;

9 **„recipient”** means a natural or legal person, public authority, entity or other entity to which personal data is disclosed, whether or not it is a third party. However, public authorities that may receive personal data in the context of a specific proceeding in accordance with Union law or the law of a Member State are not considered recipients; the processing of such data by these public authorities must comply with the data protection laws applicable according to the purposes of the processing;

10) **„third party”** means a natural or legal person, public authority, entity or body other than the data subject, controller, processor or persons who, under the authority of the controller or processor, may process personal data;

11) **„consent of data subject”** means a voluntary, specific, conscious and unequivocal demonstration of will by which the data subject, in the form of a statement or explicit affirmative action, consents to the processing of personal data concerning him;

12) **„violation of personal data protection”** means a breach of security leading to the accidental or unlawful destruction, loss, modification, unauthorized disclosure of or unauthorized access to personal data transmitted, stored or otherwise processed;

13) **„entrepreneur”** means an individual or legal entity engaged in business, regardless of legal form, including partnerships or associations engaged in regular business activities;

14) **„regulation”** means Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 (General Data Protection Regulation);

15) **„act”** means the Personal Data Protection Act of 10.05.2018;

16) **„Charter of Fundamental Rights”** stands for the Charter of Fundamental Rights of the European Union.

2. Purpose of the document.

This document is intended to define the rules of personal data processing at PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna - both as a personal data controller and processor.

Adherence to the rules set forth in the Personal Data Protection Policy and Personal Data Processing Rules is intended to guarantee the security of personal data processed by PEKO Spedycja Międzynarodowa W.Jankowski, P. Stachura Spółka Jawna in connection with its business activities.

The established principles and rules for the processing of personal data are introduced to ensure, appropriate to the degree of risk, the protection of personal data.

The processing of personal data for purposes other than those for which the data were originally collected is permitted only in cases where it is compatible with the purposes for which the personal data were originally collected. In such a case, a separate legal basis other than the legal basis that enabled the collection of personal data is not required.

In order to determine whether the purpose of the further processing of personal data is compatible with the purpose for which the data were originally collected, the controller - after fulfilling all the requirements for determining the lawfulness of the original processing - should take into account, among other things: any links between those purposes and the purposes of the intended further processing; the context in which the personal data were collected, in particular reasonable grounds for data subjects to expect further use of the data based on the nature of their relationship with the controller; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of adequate safeguards during both the original and intended further processing operation.

3. Scope of personal data processing.

Data protection principles regarding the protection of individuals' data.

In order to prevent a serious risk of circumvention, the protection of individuals should be technically neutral and should not depend on the techniques used. Thus, the entrepreneur, in addition to the technical measures implemented, undertakes acts of diligence in protecting the personal data it processes.

Within the scope of PEKO Spedycja Międzynarodowa W. Jankowski, P. Stachura Spółka Jawna activities on the Internet, individuals may be assigned Internet identifiers - such as IP addresses, cookie identifiers - generated by their devices, applications, tools and protocols,

or other identifiers. The above may result in leaving traces, which, especially in combination with unique identifiers and other information obtained by servers, can be used to create profiles and to identify individuals.

If the personal data processed by PEKO Spedycja Międzynarodowa W. Jankowski, P. Stachura Spółka Jawna do not identify an individual, PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna is not obliged to obtain additional information to identify the data subject solely to comply with the provisions of this Regulation.

However, PEKO Spedycja Międzynarodowa W. Jankowski, P. Stachura Spółka Jawna does not refuse to accept additional information from the data subject to facilitate the exercise of his rights. Identity verification should include digital identification of the data subject, for example through an authentication mechanism such as the same credentials the data subject uses to log in to online services offered by the controller..

4. Rules for processing personal data.

A. General principles.

All processing of personal data should be lawful and fair.

It should be transparent to individuals that personal data concerning them is being collected, used, viewed or otherwise processed, and to what extent that personal data is or will be processed.

The principle of transparency requires that all information and all communications related to the processing of such personal data be easily accessible and understandable, and in clear and simple language. This principle applies in particular to informing data subjects of the identity of the controller and the purposes of the processing and other information designed to ensure that the processing is fair and transparent to the individuals concerned, as well as the right of such individuals to obtain confirmation and information about the personal data processed concerning them.

Individuals should be made aware of the risks, principles, safeguards and rights associated with the processing of personal data and how to exercise their rights in connection with such processing.

In particular, the specific purposes of personal data processing should be clear, legitimate and defined at the time of collection. Personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the data retention period is kept to a strict minimum. Personal data

should be processed only in cases where the purpose of the processing cannot be reasonably achieved by other means.

To prevent personal data from being kept for longer than necessary, the controller should set a deadline for deletion or periodic review. All reasonable measures should be taken to ensure the rectification or deletion of personal data that is inaccurate. Personal data should be processed in a manner that ensures its adequate security and appropriate confidentiality, including protection against unauthorized access to and use of the data and processing equipment.

The principle of transparency requires that any information addressed to the general public or the data subject be concise, easily accessible and understandable, be formulated in clear and simple language, and, where appropriate, be further visualized. This information may be provided in electronic form, for example, via a website, when directed to the general public. This is particularly true when the large number of entities and the technological complexity of the activities make it difficult for the data subject to know and understand whether personal data pertaining to him or her is being collected, by whom and for what purpose, such as in the case of online advertising. Given that children deserve special protection, all information and communications - when the processing concerns a child - should be formulated in such clear and simple language that the child can easily understand them.

Procedures should be provided to facilitate the data subject's exercise of his or her rights under this Regulation, including mechanisms for requesting - and, when applicable, obtaining free of charge - in particular access to and rectification or erasure of personal data and the possibility of exercising the right to object.

The controller should ensure that the relevant requests can also be made electronically, in particular when personal data is processed electronically.

The controller should be obliged to respond to the requests of data subjects without undue delay - within one month at the latest, and if it does not intend to comply with such a request - to provide reasons for this.

The principles of fair and transparent processing require that the data subject be informed about the conduct of the processing operation and its purposes. The controller should provide the data subject with any other information necessary to ensure the fairness and transparency of the processing, taking into account the specific circumstances and the specific context of the processing of personal data. If personal data is collected from the data subject, he or she should also be informed whether he or she is required to provide it, and of the consequences of not doing so. This information can be provided in conjunction with

standard graphic signs that visibly, comprehensibly and legibly present the meaning of the intended processing. If the signs are presented electronically, they should be machine-readable.

Personal data must be:

(a) processed lawfully, fairly and in a manner that is transparent to the data subject ("lawfulness, fairness and transparency");

(b) collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; further processing for archival purposes in the public interest, for scientific or historical research or for statistical purposes shall not be considered incompatible with the original purposes ("purpose limitation");

(c) adequate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization");

(d) correct and updated as necessary; all reasonable steps must be taken to ensure that personal data that are inaccurate in light of the purposes for which they are processed are promptly deleted or rectified ("accuracy");

(e) kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data are processed; personal data may be kept for longer periods insofar as they will be processed exclusively for archival purposes in the public interest, for scientific or historical research purposes, or for statistical purposes pursuant to Article 89(1) of the Regulation, provided that appropriate technical and organizational measures required by this Regulation are implemented to protect the rights and freedoms of data subjects ("storage limitation");

(f) processed in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by means of appropriate technical or organizational measures ("integrity and confidentiality").

The controller is responsible for compliance with the above provisions and must be able to demonstrate compliance ("accountability").

Compliance of processing with law

1. Processing is lawful only if, and to the extent that, at least one of the following conditions is met:

(a) the data subject has consented to the processing of his or her personal data for one or more specified purposes;

(b) processing is necessary for the performance of a contract to which the data subject is a party, or to take action at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation incumbent on the controller;

(d) processing is necessary to protect the vital interests of the data subject or another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority vested in the controller;

(f) processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(4) If the processing for a purpose other than the purpose for which the personal data were collected is not based on the consent of the data subject, or on Union law or Member State law which, in a democratic society, constitute a necessary and proportionate means of securing the purposes referred to in Article 23(1) of the Regulation, the controller - in order to determine whether the processing for another purpose is compatible with the purpose for which the personal data were originally collected - shall take into account, inter alia:

(a) any relationship between the purposes for which the personal data were collected and the purposes of the intended further processing;

(b) the context in which the personal data were collected, in particular the relationship between the data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed in accordance with Article 9 of the Ordinance, or personal data relating to criminal convictions and violations of law in accordance with Article 10 of the Ordinance;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, including encryption or pseudonymization, if any.

B. Obligation to provide information on actions taken by the Personal Data Controller.

The controller shall, without undue delay - and in any case within one month of receipt of the request - provide the data subject with information on the action taken on his or her requests.

If necessary, this deadline may be extended for another two months due to the complexity of the request or the number of requests. Within one month of receipt of the request, the controller shall inform the data subject of such extension, stating the reasons for the delay. If the data subject has transmitted his request electronically, the information shall also be transmitted electronically, if possible, unless the data subject requests another form.

If the controller does not act on the data subject's request, the controller shall promptly - no later than one month after receipt of the request - inform the data subject of the reasons for the failure to act and of the possibility of lodging a complaint with the supervisory authority and pursuing legal remedies before the courts.

Information and communication and actions in connection with responding to requests from data subjects shall be free of charge.

If the data subject's requests are manifestly unreasonable or excessive, in particular due to their continuing nature, PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna may:

(a) charge a reasonable fee, taking into account the administrative costs of providing the information, conducting the communication or taking the requested action; or.

b) refuse to act on the request.

The burden is on PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna to demonstrate that the request is manifestly unreasonable or excessive in nature.

C. Obligation to notify rectification or erasure of personal data or restriction of processing.

The controller shall inform of the rectification or erasure of personal data, or restriction of processing, any recipient to whom personal data have been disclosed, unless this proves impossible or will require a disproportionate effort.

The controller shall inform the data subject of these recipients if the data subject so requests.

D. Technical and organizational measures.

Taking into account the nature, scope, context and purposes of the processing and the risk of violation of the rights or freedoms of natural persons with different probability and severity of the threat, PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna implements appropriate technical and organizational measures to ensure that the processing

is carried out in accordance with this Regulation and to be able to demonstrate this. These measures shall be reviewed and updated as necessary.

If proportionate to the processing activities, the measures referred to above shall include the implementation by the controller of appropriate data protection policies.

E. Consideration of data protection in the design phase and data protection by default

Taking into account the state of the art, the cost of implementation, and the nature, scope, context and purposes of the processing, as well as the risk of violation of the rights or freedoms of individuals with different probability of occurrence and severity of the risk resulting from the processing, PEKO Spedycja Międzynarodowa W. Jankowski, P. Stachura - both in determining the means of processing and at the time of the processing itself - shall implement appropriate technical and organizational measures, such as pseudonymization, designed to effectively implement data protection principles, such as data minimization, and to give the processing the necessary safeguards to meet the requirements of this Regulation and protect the rights of data subjects.

PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna shall implement appropriate technical and organizational measures so that, by default, only those personal data are processed that are necessary to achieve each specific purpose of processing. This obligation refers to the amount of personal data collected, the scope of their processing, the period of their storage and their availability. In particular, these measures ensure that, by default, personal data is not made available to an unspecified number of individuals without the person's intervention.

F. Basic principles to ensure the security of personal data.

To ensure the degree of security of personal data, PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna employs technical measures to:

(a) the ability to continuously ensure the confidentiality, integrity, availability and resilience of processing systems and services;

b) the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident;

c) regular testing, measurement and evaluation of the effectiveness of technical and organizational measures to ensure processing security.

G. Consideration of the risks involved in processing personal data.

In assessing whether the degree of security is adequate, particular consideration shall be given to the risks inherent in the processing, in particular those arising from the accidental or unlawful destruction, loss, modification, unauthorized disclosure of or unauthorized access to personal data transmitted, stored or otherwise processed.

H. Methods to limit the processing of personal data.

Among the methods to restrict the processing of personal data may be: temporarily transferring selected personal data to another processing system, preventing users from accessing selected data, or temporarily removing published data from a website. In automated filing systems, processing should generally be restricted by technical means so that personal data are not subject to further processing or alteration. The fact that processing of personal data is restricted must be clearly indicated in the system.

5. Responsibilities of the Personal Data Administrator

1. Obligation to transfer personal data, to the person to whom the data refers.

Information about the processing of personal data concerning the data subject must be provided to the data subject at the time of data collection, or, if the data is not obtained from the data subject but from another source, within a reasonable period of time, as the case may be.

If the personal data can be lawfully disclosed to another recipient, the data subject must be informed at the time of the first disclosure to that recipient. If the controller plans to process personal data for a purpose other than the purpose for which the personal data was collected, the controller should inform the data subject of the other purpose and provide him with other necessary information before such further processing. If the data subject cannot be told the origin of the personal data because different sources were used, the information should be provided in general terms.

In order to gain greater control over his or her data through automated processing of personal data, the data subject should also be able to receive personal data concerning him or her that he or she has provided to the controller in a structured, commonly used, machine-readable and interoperable format and send it to another controller.

This right applies in cases where the data subject has provided the personal data with his or her own consent or where the processing is necessary for the performance of a contract. It should not apply if the processing is based on a legal basis other than consent or contract.

The data subject's right to send or receive his personal data does not impose an obligation on the controller to maintain or implement technically compatible processing systems.

If a specific set of personal data relates to more than one data subject, the right to receive personal data should not cause prejudice to the rights and freedoms of other data subjects. In addition, this right should be without prejudice to the data subject's right to cause the personal data to be erased and should not, in particular, result in the erasure of personal data relating to the data subject that the data subject has provided for the performance of the contract, if and to the extent that such personal data is necessary for the performance of the contract. Insofar as technically possible, the data subject should have the right to have the personal data sent by one controller directly to another controller.

A. Information provided when collecting data from a data subject.

(1) If the personal data of a data subject is collected from the data subject, the controller shall provide the data subject with all of the following information when obtaining the personal data:

(a) his or her identity and contact information and, when applicable, the identity and contact information of his or her representative;

(b) when applicable, the contact information of the Data Protection Officer;

(c) the purposes of personal data processing and the legal basis for processing;

(d) information about the recipients of personal data or categories of recipients, if any.

(2) In addition to the information referred to above, when obtaining personal data, the controller shall provide the data subject with the following other information necessary to ensure the fairness and transparency of the processing:

(a) the period for which the personal data will be kept and, when this is not possible, the criteria for determining this period;

(b) information about the right to request from the controller access to, rectification, erasure or restriction of processing of personal data concerning the data subject, or the right to object to processing, as well as the right to data portability;

(c) information about the right to lodge a complaint with a supervisory authority;

(d) information on whether the provision of personal data is a statutory or contractual requirement or a condition for entering into a contract, and whether the data subject is obliged to provide such data and the possible consequences of failing to do so;

(3) If the controller plans to further process the personal data for a purpose other than the purpose for which the personal data were collected, the controller shall, prior to such further processing, inform the data subject of such other purpose and provide him/her with all other relevant information referred to in subparagraph (2).

(4) Paragraphs (1), (2) and (3) shall not apply if, and to the extent that, the data subject already has this information.

B. Information provided when personal data is obtained by means other than from the data subject

(1) If the personal data was not obtained from the data subject, the controller shall provide the data subject with the following information:

(a) his or her identity and contact information and, when applicable, the identity and contact information of his or her representative;

(b) where applicable, the contact information of the data protection officer;

(c) the purposes of the processing for which the personal data are to be used, and the legal basis for the processing;

(d) the categories of personal data involved;

e) information about the recipients of the personal data or categories of recipients, if any.

(2) In addition to the information referred to in paragraph (1), the controller shall provide the data subject with the following information necessary to ensure the fairness and transparency of the processing to the data subject:

(a) the period for which the personal data will be kept, and, when this is not possible, the criteria for determining this period;

b) information on the right to request from the controller access to, rectification, erasure or restriction of processing of personal data concerning the data subject, and the right to object to processing, as well as the right to data portability;

(c) information about the right to lodge a complaint with a supervisory authority;

(d) the source of the personal data and, where applicable, whether it comes from publicly available sources;

(3) The information referred to in (1) and (2) shall be provided by the controller:

(a) within a reasonable period of time after the acquisition of personal data - within one month at the latest - given the specific circumstances of the processing of personal data;

(b) if the personal data are to be used for communication with the data subject - at the latest at the first such communication with the data subject; or

(c) if it is planned to disclose the personal data to another recipient - at the first disclosure at the latest.

(4) If the controller plans to further process the personal data for a purpose other than the purpose for which the data were obtained, the controller shall, prior to such further processing, inform the data subject of that other purpose and provide him with all other relevant information referred to in paragraph (2).

(5) Paragraphs 1- 4 shall not apply when - and to the extent that:

(a) the data subject already has this information;

(b) the provision of such information proves impossible or would require a disproportionate effort; in particular, in the case of processing for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) of the Regulation, or insofar as the obligation referred to in point 1 of this Article is likely to render impossible or seriously impede the achievement of the purposes of such processing. In such cases, the controller shall take appropriate measures to protect the rights and freedoms and legitimate interests of the data subject, including making the information available to the public;

(c) the acquisition or disclosure is expressly governed by Union law or the law of the Member State to which the controller is subject, providing for appropriate measures to protect the legitimate interests of the data subject; or

(d) the personal data must remain confidential in accordance with an obligation of professional secrecy under Union or Member State law, including a statutory obligation of secrecy.

2. Obligation to verify personal data, before sharing it.

The controller should use all reasonable means to verify the identity of the data subject requesting access, particularly in the context of Internet services and Internet identifiers. The controller should not retain personal data for the sole purpose of responding to possible requests.

3. Obligation to determine the likelihood and severity of the risk of violation of rights or freedoms in the case of violations.

The likelihood and seriousness of the risk of violation of the rights or freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. The risk should be estimated on the basis of an objective assessment that determines whether there is a risk or high risk associated with the processing operations.

In order to maintain security and prevent non-compliant processing, the controller or processor should assess the risks inherent in the processing and implement measures - such as encryption - that minimize those risks. Such measures should ensure an appropriate level of security, including confidentiality, and take into account the state of the art and the cost of their implementation in relation to the risk and nature of the personal data to be protected.

In assessing data security risks, consideration should be given to the risks associated with the processing of personal data - such as accidental or unlawful destruction, loss, modification, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise processed - and which may, in particular, lead to physical harm, property damage or non-property damage.

4. Implementation of appropriate technical and organizational measures.

The protection of the rights and freedoms of individuals in connection with the processing of personal data requires the implementation of appropriate technical and organizational measures to ensure compliance with the requirements of data protection legislation.

In order to be able to demonstrate compliance with data protection laws, the controller shall implement measures that comply in particular with the principle of data protection by design and the principle of data protection by default.

If applications, services and products are developed, designed, selected and used that either rely on the processing of personal data or process personal data in order to carry out their task, the manufacturers of such products, services and applications should be encouraged to take into account the right to personal data protection when developing and designing such products, services and applications, and with due regard to the state of the art, ensure that controllers and processors are able to meet their data protection obligations.

6. Entrustment of personal data processing.

In order to ensure compliance with the requirements of the Ordinance in the case of processing to be carried out by a processor on behalf of the controller, the controller should, when entrusting processing activities to a processor, use only processors that provide sufficient guarantees - in particular in terms of expertise, reliability and resources - of the implementation of technical and organizational measures that meet the requirements of the Ordinance, including processing security requirements.

The processor's use of an approved code of conduct or an approved certification mechanism may serve as an element demonstrating compliance with the controller's obligations. Processing by a processor should be governed by a contract or other legal instrument that is subject to Union or Member State law, binds the processor to the controller, specifies the subject matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, and which should take into account the specific tasks and obligations of the processor in the context of the planned processing and the risk of violation of the rights or freedoms of the data subject. The controller and the processor may decide to use an individual contract or standard contractual clauses that have been adopted directly by the Commission or that have been adopted by the supervisory authority in accordance with the consistency mechanism and subsequently adopted by the Commission. Upon termination of processing on behalf of the controller, the processor should, as decided by the controller, return or delete the personal data, unless Union law or the law of the Member State to which the processor is subject imposes an obligation to retain the personal data.

Processing entity

(1) If the processing is to be carried out on behalf of the controller, the controller shall only use the services of such processors that provide sufficient guarantees to implement appropriate technical and organizational measures so that the processing meets the requirements of the Regulation and protects the rights of the data subjects.

(2) A processor shall not use the services of another processor without the prior specific or general written consent of the controller. In the case of general written consent, the processor shall inform the controller of any intended changes regarding the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(3) Processing by a processor shall be carried out on the basis of a contract or other legal instrument that is subject to Union or Member State law and binds the processor and the

controller, specifies the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller. In particular, this contract or other legal instrument stipulates that the processor:

(a) process personal data only on the documented instructions of the controller - which shall also apply to transfers of personal data to a third country or an international organization - unless such obligation is imposed by Union law or the law of a Member State to which the processor is subject, in which case the processor shall inform the controller of this legal obligation prior to the start of processing, unless such law prohibits the provision of such information for reasons of important public interest;

(b) shall ensure that persons authorized to process personal data are bound to secrecy or are subject to the relevant legal obligation of secrecy;

(c) take all measures required under Article 32 of the Regulation;

(d) complies with the conditions for the use of another processor referred to in items. 2 i 4;

(e) taking into account the nature of the processing, assist the controller, as far as possible, through appropriate technical and organizational measures, in fulfilling its obligation to respond to the data subject's requests for the exercise of his or her rights set forth in Chapter III;

(f) taking into account the nature of the processing and the information available to it, assist the controller in complying with the obligations set forth in Articles 32-36 of the Regulation;

(g) upon termination of the processing services, depending on the decision of the controller, delete or return to the controller any personal data and delete any existing copies thereof, unless Union or Member State law prescribes the retention of personal data;

(h) shall make available to the controller all information necessary to demonstrate compliance with the obligations set forth in this Article, and shall allow and contribute to audits, including inspections, by the controller or an auditor authorized by the controller.

In connection with the obligation set forth in point (h) of the first paragraph, the processor shall immediately inform the controller if, in its opinion, the order issued to it constitutes a violation of this Regulation or other Union or Member State data protection legislation.

(4) If a processor uses another processor to carry out specific processing activities on behalf of the controller, the same data protection obligations shall be imposed on that other processor under a contract or other legal act governed by Union or Member State law as in the contract or other legal act between the controller and the processor referred to in point. 3,

in particular the obligation to provide sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing complies with the requirements of this Regulation. If this other processor fails to comply with its data protection obligations, the full liability to the controller for compliance with the obligations of this other processor shall rest with the original processor.

(5) Sufficient guarantees referred to in items. 1 and 4 of this Article may be demonstrated by the processor, among others, through the application of an approved code of conduct referred to in Article 40 of the Ordinance or an approved certification mechanism referred to in Article 42 of the Ordinance.

7. Rights of persons whose personal data are processed.

A. Right to rectification of personal data and right to be forgotten.

Every individual should have the right to rectification of personal data concerning him or her and the right to "be forgotten" if the retention of such data violates the Regulation, Union law or the law of the Member State to which the controller is subject.

In particular, the data subject should have the right to have his or her personal data erased and no longer processed if the data is no longer necessary for the purposes for which it was collected or otherwise processed, if the data subject has withdrawn consent or if he or she has objected to the processing of personal data concerning him or her, or if the processing of his or her personal data is otherwise not in compliance with this Regulation.

This right is relevant in cases where the data subject gave his or her consent as a child, when he or she was not fully aware of the risks involved in the processing, and later wishes to delete such personal data, particularly from the Internet.

However, the continued retention of personal data should be considered lawful if it is necessary for the exercise of freedom of expression and information, for the fulfillment of a legal obligation, for the performance of a task carried out in the public interest or in the exercise of public authority entrusted to the controller, for reasons of public interest in the field of public health, for archival purposes in the public interest, for scientific or historical research or statistical purposes, or for the establishment, assertion or defense of claims.

In order to strengthen the right to "be forgotten" on the Internet, the right to erasure should be expanded by requiring a controller who has made such personal data public to inform controllers who process such personal data to delete any links to, copies of, or replications of such personal data.

In fulfilling this obligation, the controller should take reasonable measures, taking into account available technologies and the means available to it, including available technical means, to inform controllers who process personal data of the data subject's request.

B. Right to erasure of data ("right to be forgotten")

1. The data subject has the right to request from the controller the immediate erasure of personal data concerning him/her, and the controller is obliged to erase the personal data without undue delay if one of the following circumstances applies:

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

(b) the personal data were processed unlawfully;

(c) the personal data must be deleted in order to comply with a legal obligation under Union law or the law of a Member State to which the controller is subject;

(2) If the controller has made the personal data public, and is required to erase the personal data under subparagraph (1), the controller shall, taking into account the available technology and the cost of implementation, take reasonable measures, including technical measures, to inform the controllers processing the personal data that the data subject requests that the controllers erase any links to the data, copies of the personal data or replications of the personal data.

(3) Paragraphs (1) and (2) shall not apply to the extent that the processing is necessary:

(a) to exercise the right to freedom of expression and information;

(b) for compliance with a legal obligation requiring processing under Union law or the law of a Member State to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for archival purposes in the public interest, for scientific or historical research purposes, or for statistical purposes in accordance with Article 89(1) of the Regulation, insofar as it is likely that the right referred to in para. 1, will prevent or seriously impede the purposes of such processing; or

(e) for the establishment, investigation or defense of claims.

C. Right to rectify personal data.

The data subject has the right to request from the controller the prompt rectification of personal data concerning him/her that is inaccurate. Taking into account the purposes of the

processing, the data subject has the right to request the completion of incomplete personal data, including by providing an additional statement.

D. Right to object

If personal data are processed for direct marketing purposes, the data subject should have the right to object at any time, free of charge, to such processing, whether primary or further - including profiling, insofar as it is related to direct marketing. This right should be clearly communicated to the data subject and should be presented clearly and separately from any other information. If the data subject objects to processing for direct marketing purposes, the personal data must no longer be processed for such purposes.

At the latest on the occasion of the first communication with the data subject, the data subject shall be clearly informed of the rights referred to above, and shall be presented clearly and separately from any other information

E. Right to file a complaint

Each data subject has the right to lodge a complaint with a supervisory authority and the right to an effective remedy before a court - in accordance with applicable law.

F. Right of access to personal data

1. The data subject is entitled to obtain from PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna confirmation as to whether personal data concerning him or her is being processed, and if this is the case, he or she is entitled to obtain access to it and the following information:

(a) the purposes of the processing;

(b) the categories of personal data involved;

c) information about the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

(d) where possible, the intended period of storage of personal data, and where this is not possible, the criteria for determining this period;

e) information on the right to request rectification, erasure or restriction of the processing of personal data concerning the data subject, and to object to such processing;

(f) information about the right to lodge a complaint with a supervisory authority;

(g) if the personal data was not collected from the data subject - any available information about its source.

(2) PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna shall provide the data subject with a copy of the personal data subject to processing. For any subsequent copies requested by the data subject, PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna may charge a reasonable fee based on administrative costs. If the data subject requests a copy by electronic means, and unless he or she indicates otherwise, the information shall be provided by common electronic means.

(3) The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

G. Right to restrict processing

(1) The data subject shall have the right to request that PEKO Spedycja Międzynarodowa W. Jankowski, P. Stachura Spółka Jawna restrict processing in the following cases:

(a) the data subject disputes the correctness of the personal data - for a period of time allowing to verify the correctness of the data;

(b) the processing is unlawful, and the data subject objects to the erasure of the personal data, requesting instead that the use of the data be restricted;

(c) PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna no longer needs the personal data for the purposes of processing, but the data are needed by the data subject to establish, assert or defend claims.

(2) If processing has been restricted pursuant to subsection (1), such personal data may be processed, with the exception of storage, only with the consent of the data subject, or to establish, assert or defend claims, or to protect the rights of another natural or legal person, or for compelling reasons of public interest of the Union or a Member State.

(3) Before lifting a restriction on processing, the controller shall inform the data subject who requested the restriction under paragraph (1).

H. Right to data portability

(1) The data subject shall have the right to receive in a structured, commonly used machine-readable format the personal data concerning him or her that he or she has provided to the controller, and shall have the right to send such personal data to another controller without hindrance from the controller to whom the personal data were provided, if the processing is carried out by automated means.

(2) In exercising the right to data portability under subsection (1), the data subject shall have the right to request that the personal data be sent by the controller directly to another controller, insofar as this is technically possible.

(3) The right referred to in Section 1 shall not adversely affect the rights and freedoms of others..

8. Handling of violations.

A. Notification in case of violations.

In the absence of an adequate and prompt response, a personal data protection breach may result in physical harm, property damage or non-property damage to individuals, such as loss of control over their own personal data or restriction of rights, discrimination, identity theft or forgery, financial loss, unauthorized reversal of pseudonymization, damage to reputation, breach of confidentiality of personal data protected by professional secrecy, or any other significant economic or social damage.

For the above reasons, as soon as PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna discovers a violation of personal data protection, it should report it to the supervisory authority without undue delay, if feasible, no later than within 72 hours PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna is able to demonstrate, in accordance with the principle of accountability, that the violation is unlikely to cause a risk of violation of the rights or freedoms of individuals.

If the notification cannot be made within 72 hours, the notification should be accompanied by an explanation of the reasons for the delay, and the information may be provided gradually, without further undue delay.

PEKO Spedycja Międzynarodowa W.Jankowski, P.Stachura Spółka Jawna should, without undue delay, inform the data subject of a personal data protection breach if it may cause a high risk of infringement of the rights or freedoms of that person, so as to enable that person to take the necessary preventive measures. Such information should include a description of the nature of the personal data protection breach and recommendations for the individual concerned to minimize potential adverse effects. The information should be provided to data subjects as soon as reasonably practicable, in close cooperation with the supervisory authority, respecting guidance provided by the supervisory authority or other relevant authorities, such as law enforcement. For example, the need to minimize the immediate risk of harm will require informing data subjects immediately, while the implementation of

appropriate measures against the same or similar data protection breaches may justify later information.

B. **Ensuring an adequate level of security.**

Ensure that all appropriate technical protection measures and all appropriate organizational measures have been implemented to immediately identify the personal data breach and promptly notify the supervisory authority and the data subject. Whether notification has been made without undue delay should be determined taking into account, in particular, the nature and gravity of the personal data protection breach, its consequences and adverse effects on the data subject. Such notification may result in the intervention of the supervisory authority, in accordance with its tasks and powers set forth in the Regulation.

C. Reporting a data breach to the supervisory authority

1. In the event of a violation of personal data protection, PEKO Spedycja Międzynarodowa W. Jankowski, P. Stachura Spółka Jawna shall, without undue delay - if possible, no later than 72 hours after the discovery of the violation - report it to the competent supervisory authority, unless the violation is unlikely to result in a risk of violation of the rights or freedoms of individuals. A notification submitted to the supervisory authority after 72 hours shall be accompanied by an explanation of the reasons for the delay.

(2) The processor shall, upon discovery of a personal data breach, without undue delay, notify the controller of the breach.

(3) The notification referred to in Section 1 shall at least:

(a) describe the nature of the personal data protection breach, including, if possible, the categories and approximate number of data subjects and the categories and approximate number of personal data records affected by the breach;

(b) contain the name and contact information of the Data Protection Officer or the designation of another point of contact from whom more information can be obtained;

c) describe the possible consequences of the personal data breach;

(d) describe the measures applied or proposed by the controller to remedy the personal data protection breach, including, if applicable, measures to minimize its possible negative consequences.

(4) If - and to the extent that - the information cannot be provided at the same time, it may be provided successively without undue delay

(5) The controller shall document any personal data breach, including the circumstances of the personal data breach, its consequences and the remedial action taken. This documentation must allow the supervisory authority to verify compliance with the law.

D. Notifying the data subject of a personal data breach

(1) If a personal data protection violation is likely to cause a high risk of violation of the rights or freedoms of natural persons, it shall notify the data subject of such violation without undue delay.

(2) The notice referred to in paragraph (1) of this Article shall, in clear and simple language, describe the nature of the personal data protection violation and shall contain at least the information and measures referred to in Article 33(3)(b), (c) and (d) of the Regulation.

(3) The notification referred to in paragraph (1) shall not be required in the following cases:

(a) appropriate technical and organizational protection measures have been implemented and these measures have been applied to the personal data affected by the violation, in particular measures such as encryption to prevent reading by unauthorized persons from accessing such personal data;

(b) measures have subsequently been applied to eliminate the likelihood of a high risk of violation of the rights or freedoms of the data subject referred to in para. 1;

(c) it would require a disproportionately large effort. In such a case, a public notice shall be issued or a similar measure shall be taken by which the data subjects are informed in an equally effective manner.

(4) If PEKO Spedycja Międzynarodowa W. Jankowski, P. Stachura Spółka Jawna has not yet notified the data subject of a personal data breach, the supervisory authority - taking into account the likelihood that this personal data breach will result in a high risk - may require it to do so, or may determine that one of the conditions referred to in point 3 has been met.