


Internal Regulation on Personal Data Processing			Doc. No. 12066	Version 02	Language EN	
Country	SK	Directive	1 st Release 2024-MAR-27	Last Update 2024-NOV-29	Valid From 2024-DEC-10	
Target Group: ALL			Owner: Managing Director SK			

Table of contents

1	General Provisions	2
1.1	Purpose	2
1.2	Scope and application of Directive	2
1.3	Company's position with regard to personal data processing	3
1.4	Information systems and authorisations to process data in those systems	3
2	Basic principles of personal data processing	4
2.2	Legality, fairness and transparency	4
2.3	Purpose limitation	4
2.4	Minimising scope of data	5
2.5	Principle of justice	5
2.6	Minimising data retention periods	5
2.7	Integrity and confidentiality	5
2.8	Responsibility	6
2.9	Processing special categories of personal data	6
3	Data subject's rights	7
3.1	Right to information	7
3.2	Right of access to personal data	9
3.3	Right to rectification	9
3.4	Right to erasure	9
3.5	Right to restrict processing	10
3.6	Right to data portability	10
3.7	Right to object	10
3.8	Automated individual decision-making, profiling included	11
3.9	Exercising data subjects' rights	11
4	Impact assessment and prior consultation	13
5	Personal data security	13
5.1	Adequacy of security measures	13
5.2	Notification of personal data breaches	14
6	Other entities involved in personal data processing	15
6.1	Personal data provision	15
6.2	Use of processors	15
7	Data Protection Officer (DPO)	15
8	Personal data destruction	15
9	Final Provisions	15
10	Glossary of terms	16
11	History of Changes	17
12	Annex 3 – INFORMATION ON JOB SEEKERS' PERSONAL DATA PROCESSING in cargo-partner SR, s.r.o.	18
13	Annex 4 – APPLICANT'S CONSENT TO THE PROCESSING OF PERSONAL DATA IN JOB SEEKERS DATABASE	22

14	Annex 5 – INFORMATION ON EMPLOYEES’ PERSONAL DATA PROCESSING	23
15	Annex 6 – INFORMATION ON BUSINESS PARTNERS, CONTACT PERSONS, SHIPMENT SENDERS AND RECIPIENTS AND OTHER PERSONS’ PERSONAL DATA PROCESSING,	29
16	Annex 7 – NOTIFICATION OF PERSONAL DATA SECURITY BREACH (SPECIMEN)	35

1 General Provisions

1.1 Purpose

- A. Personal data processing is an integral part of any business activity performance. The compliance of processing operations with legal regulations, in particular 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 (General Data Protection Regulation) (hereinafter referred to as the “**GDPR**”), Act No. 18/2018 Coll. on the Protection of Personal Data, as amended (hereinafter referred to as “**the Act**”), as well as other relevant legislation, is a fundamental obligation of information system processors and controllers.
- B. Cargo-partner SR, s.r.o., registered office: Kopčianska 92, 851 01 Bratislava – City District Petržalka, Company ID No.: 31 358 152, entered in the Business Register maintained by the Bratislava III City Court, Part. SRO, Entry No.: 5741/B (hereinafter referred to as the “**Company**”),
- Respects the trust of its employees, customers, suppliers and any others of those the personal data of whom it processes;
 - Recognises the importance of protecting the personal data it processes; and
 - It shall continuously take the steps necessary and effective for ensuring compliance and update them as necessary.
- C. For these reasons, the Company adopts this internal Data Protection Directive (hereinafter referred to as the “**Directive**”) drawn up in accordance with the provisions of the GDPR that regulates the processing of personal data within the Company and determines the rights and obligations of persons involved in the processing i.e. data subjects and persons authorised to handle personal data on behalf of the Company.

1.2 Scope and application of Directive

- A. The Directive shall apply to operations relating to the processing of personal data carried out by the Company from 25 May 2018.
- B. The Directive does not apply to personal data processing that is not covered by the GDPR and the Act.
- C. The GDPR is a general legal regulation of the European Union designed to protect personal data. Moreover, there are some other legal regulations that apply to the performance of the Company’s business activities and to that related processing of personal data, e.g. Act No. 311/2001 Coll., Labour Code, Act No. 124/2006 Coll. on occupational health and safety, Act No. 431/2002 Coll. on accounting, Act No. 351/2011 Coll. on electronic communications, as amended, etc.
- D. The terms used in the Directive have the same meaning as the same terms defined in Article 4 of the GDPR; **the meaning of the basic terms is specified in Point 10 of hereof (Glossary of Terms).**

1.3 Company's position with regard to personal data processing

- A. In connection with personal data processing, the Company has the status of a controller within the meaning of Article 4, point 7 of the GDPR.
- B. The Company is not considered a controller if it obtains personal data accidentally without prior determination of the purposes and means of processing, in which case the GDPR does not apply to it. These may be situations where the Company is provided with personal data in mistake or it is provided with such personal data that it has not requested and has no interest in further processing for any purpose. The storage of this data, e.g. due to their return to the authorised person or their deletion within a reasonable period of time, does not constitute the processing of the personal data falling within the scope of the GDPR.
- C. The Company is a member of an international group of companies called cargo-partner and this is part of an international group of companies called nippon express, and there may be sharing or joint processing of personal data with other entities within such a group of companies. The Company shall provide data subjects with transparent information regarding the legitimate interests of the processing given¹, personal data recipients or categories of recipients or third countries to which the personal data is to be transferred.²

1.4 Information systems and authorisations to process data in those systems

- A. Based on the purpose of personal data processing, such processing is divided among several information systems in the Company.
1. **Employees/Human resources & wages**
 2. **Internal administrative purposes**
 3. **Security**
 4. **Contractual relations with business partners**
 5. **Accounting agenda**
 6. **Corporate agenda**
 7. **Judicial and Dispute Agenda**
 8. **Mail sent and received**
 9. **Marketing**
 10. **Whistle-blowing**
 11. **Personal data protection**
 12. **Registry management**
- B. Detailed information on individual systems, purpose and legal basis for the processing of personal data in them is contained in the document **Records of Controller's Processing Activities**, which forms **Annex 1 to the Directive**.
- C. The persons authorised to process personal data on behalf of the Company may carry out operations processing data subjects' personal data in the information system and its subsystems to the following extent:

¹ Recital 48, GDPR: "Controllers that are part of a group of undertakings or institutions linked to a central entity may have a legitimate interest in the transfer of personal data within the group of undertakings for internal administrative purposes, the processing of personal data of clients or employees included. This is without prejudice to the general principles for the transfer of personal data within a group of undertakings to an undertaking located in a third country."

² Article 13, par. 1 (d), (e) and (f) of GDPR.

Degrees of authorisation:

- Degree 1= D1 Permission to become familiar with personal data
- Degree 2= D2 Authorisation to collect, record, and modify personal data
- Degree 3= D3 Authorisation for any processing operations (including personal data destruction, provision and disclosure)

Each level of authorisation (appointment) corresponds to the job position of a particular employee in accordance with the “**Matrix of Personal Data Processing Authorisations of Employees**” document, which forms **Annex 2 to the Directive**.

2 Basic principles of personal data processing

- A. In its Article 5, the GDPR regulates the basic principles of personal data processing. The Company continues ensuring that all processing operations are carried out in accordance with all the principles set out below.

2.2 Legality, fairness and transparency

- A. The Company processes data subjects’ personal data lawfully, fairly and transparently.
- B. The legal method of processing means that the processing of personal data is based on one of the legal bases of the processing referred to in Articles 6 to 11 and 89 of the GDPR.
- C. Fairness and transparency means that the Company provides the data subjects whose personal data is processed with clear and comprehensible information about the processing conditions and the rights they have in this regard. In addition to informing them about their rights, data subjects shall be informed, to the extent legally required, of the specificities of the processing such as the purposes such data is processed for and the legal basis of its processing. The scope of the obligation to provide information is regulated in Articles 13 and 14 of the GDPR and, at the data subject’s request, in Article 15 of the GDPR. It follows from these provisions that the right of data subjects to be provided with information is not absolute and in some cases the Company is not explicitly obliged to inform them.

2.3 Purpose limitation

- A. The Company collects personal data for specified, explicitly stated and legitimate purposes. The data given may not be further processed in a way that is incompatible with the purposes given. However, further processing for a purpose other than that for which the personal data was collected is permitted under certain conditions, i.e. even if the Company obtains personal data for a specific purpose, subject to specified conditions, it may also process the data for a purpose other than the original one (“**compatibility test**”).
- B. Further processing for the purposes of archiving in the public interest, for the purposes of scientific or historical research or for statistical purposes is considered compatible with the original purpose within the meaning of the GDPR. For this purpose, the Company will provide adequate safeguards for data subjects’ rights and freedoms.

2.4 Minimising scope of data

A. The personal data processed by the Company is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. For this purpose, the Company carried out an audit of personal data processing before the GDPR entered into force. Moreover, it continuously monitors its processing operations. The continuous monitoring has been introduced in order to be able to demonstrate that all processed personal data is necessary for achieving the purposes of the processing pursued.

2.5 Principle of justice

- A. The Company makes reasonable efforts to ensure that the personal data processed by the Company is correct and updated as necessary. The Company ensures that the inaccurate personal data is erased or corrected without delay. Data subjects are obliged to provide the Company with correct personal data in all circumstances and to update this data effectively (e.g. in writing, e-mail communication included) for the Company, e.g. if it changes, for example.
- B. The Company assumes that the personal data provided by data subjects is true, up-to-date, complete and correct up to the moment the notification of a change in such data is provided by the data subject. In such a case, the Company shall immediately arrange for relevant personal data amendment, completion or correction.

2.6 Minimising data retention periods

- A. The Company retains personal data in a form that allows the identification of data subjects for no longer than necessary for the purposes for which personal data is processed. If personal data is processed for several purposes, the Company is entitled to process it for as long as any of such purposes lasts. Personal data may be retained for longer periods insofar as it is processed solely for archiving purposes in the public interest, for the purpose of scientific or historical research or for statistical purposes. In such a case, the Company shall ensure that appropriate technical and organisational measures are taken to protect the data subjects' rights and freedoms.
- B. Retention periods (i.e. periods of saving) may, in some cases, result from special regulations. However, some specific provisions only provide for a minimum statutory retention period, while retention periods may be longer in given cases. The principle of minimising data retention periods allows the processing of personal data to continue after retention periods for some other specified purposes. These are archiving purposes in the public interest, purposes of scientific or historical research and statistical purposes set out in Article 89 of the GDPR.

2.7 Integrity and confidentiality

- A. The Company ensures that personal data is processed in a manner that ensures the adequate security of personal data, including protection against its unauthorised or unlawful processing and against accidental loss, destruction or damage, by means of appropriate technical or organisational measures (so-called "security measures").
- B. This principle is complemented by other obligations relating to personal data security which are dealt with by the GDPR in separate Section 2, Chapter IV, namely in Articles 32 to 34 of the GDPR. The principle of integrity and confidentiality is further explained in Article 5 below.

2.8 Responsibility

- A. The Company is responsible for the processing of personal data in accordance with the above principles and takes measures to demonstrate the compliance of each processing operation. For this purpose, it, for instance, prepares written documents in which it is stated that all the aspects of processing operations within the Company have been internally reviewed, with the result of such a review being the compliance with the GDPR provisions. The obligation to demonstrate the compliance is connected exclusively with the competent Personal Data Protection Authority.
- B. In accordance with the principle of responsibility, the Company may demonstrate compliance with the basic principles of personal data processing, e.g. in one of the following ways (if applicable to the Company):
- a) Adopting and adhering to the Directive;
 - b) Entering into contracts with processors or joint controllers under Article 26 or 28 of the GDPR;
 - c) Keeping records of processing activities under Article 30 GDPR;
 - d) Providing assistance to the competent Personal Data Protection Authority in connection with the performance of its tasks and exercising of its powers under Article 31 of the GDPR;
 - e) Taking appropriate security measures under Article 32 of the GDPR;
 - f) Conducting an impact assessment and, where necessary, prior consultation under the Articles 35 and 36 of the GDPR;
 - g) Training staff in the field of personal data protection;
 - h) If necessary, appointing a person in charge of personal data protection under the Articles 37 to 39 of the GDPR;
 - i) Complying with the rules and adequate safeguards for cross-border personal data transfers to third countries or international organisations;
 - j) Complying with approved certification mechanisms, seals or marks as referred to in Article 42 et seq. of the GDPR.
- C. The Company makes reasonable efforts to ensure personal data protection through such data protection being specifically designed (“data protection by design”) and default (“data protection by default”).
- D. Personal data protection by design means that the Company, taking into account various aspects of personal data processing (e.g. latest knowledge, nature, the scope and purposes of such processing, risks connected with data subject’s rights), will take appropriate technical and organisational measures and provide adequate safeguards to protect personal data before the processing starts. These are then continuously adapted to the current conditions of processing.
- E. Personal data protection by default means that the Company ensures that only personal data necessary for each specific purpose of processing is processed. It shall also ensure that personal data is not by default accessible to an unlimited number of natural persons without such natural persons’ intervention.

2.9 Processing special categories of personal data

- A. The GDPR special category of personal data (known as “sensitive data”) is included in the personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Furthermore, as sensitive personal data the GDPR also explicitly mentions genetic data, biometric data for the individual identification of a natural person, data concerning health or data relating to a natural person’s sexual life or sexual orientation. According to Article 9, par. 1 of the GDPR, there is a general prohibition on such data processing, which does not apply only if the conditions set out in Article 9, par. 2 of the GDPR are met.

- B. Unlike the previous regulation, national identification numbers and personal data relating to criminal convictions and offences are not considered to be sensitive data. Similarly, a photograph is no longer considered to be sensitive data and therefore a usual security camera record or a copy of an identity document, the photograph on such a document included, do not fulfil this condition.
- C. When processing personal data, the Company may also come into contact with sensitive data. This will, in particular, be data relating to health for employment purposes.
- D. Sensitive data may be processed for the purpose of fulfilling the controller's or data subject's obligations and exercising their special rights in the field of labour law and social security and social protection law. The Company is entitled to process sensitive data for employment purposes even without the data subject's consent. If the Company processes sensitive data on the basis of such a subject's consent, it shall obtain explicit consent from the data subject for this effect.

3 Data subject's rights

3.1 Right to information

- A. Transparency is one of the basic principles of personal data processing. The Company therefore implements measures in its internal procedures to provide data subjects with information regarding the processing. The legal framework for providing information to the data subject is stipulated as follows:
- The information shall be provided in a concise, transparent, intelligible and easily accessible form; it shall be phrased in a clear and simple manner;
 - The information may be submitted in writing, electronically or by other means or orally, if requested;
 - The information shall be provided free of charge, in the event of data subjects' unjustified or unreasonable requests, the Company is entitled to charge a reasonable fee or not to act;
 - The Company is entitled to request the provision of additional information necessary for confirming the identity of the data subject given.
- B. The Company is entitled to fulfil its obligation to provide information under the Articles 13 and 14 of the GDPR in any appropriate and demonstrable manner, regardless of the form of the information provided. Based on the circumstances of the processing, the Company may choose to provide this information, for example by means of the link to its website, electronically via the web, in a separate pop-up window, physically in the printed form, incorporated in contractual documentation or general terms and conditions, through certified mechanisms, marks or seals, by its sending to the data subject's e-mail or postal address or orally or in writing.

Scope of obligation to provide information

- C. Where the data subject's personal data is collected from such a data subject, the Company shall provide the data subject with all of the following information:
- Controller's identity and contact details and, where applicable, controller's representative's identity and contact details;
 - Data protection officer's contact details, if any;
 - Purpose of the processing for which the personal data is intended as well as the legal basis for such processing;
 - If the processing is based on Article 6, par. 1(f), the legitimate interests pursued by the controller or by a third party;
 - Personal data recipients or categories of such recipients, if any;

- f) Where applicable, one is to inform on the controller's intention to transfer personal data to a third country or international organisation and on the existence or absence of the Commission's adequacy decision or, in the case of transfers referred to in Article 46 or 47 or in Article 49, par. 1 (2) on the reference to appropriate or adequate safeguards and means for obtaining a copy of those or where they have been provided.
- D. Apart from the information in Art. 6.3, the Company shall provide the data subject with the following additional information when collecting personal data where it is necessary to ensure fair and transparent processing:
- a) Period for which the personal data will be stored or, if this is not possible, the criteria for determining that period;
 - b) Existence of the right to ask the controller for access to and rectification or erasure of data subject's personal data or for the restriction of such personal data processing, or the right to object to processing, as well as the right to data portability;
 - c) Where processing is based on Article 6, par. 1(a) or Article 9 par. 2(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - d) Right to lodge a complaint with a supervisory authority;
 - e) Information on whether the provision of personal data is a legal or contractual requirement or a requirement necessary for entering into a contract, whether the data subject is obliged to provide their personal data, as well as the possible consequences of not providing such data;
 - f) Existence of automated decision-making, including profiling, referred to in Article 22, par. (1) and (4) 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 given.
- E. **Annex 3 to this Directive is the Information on the processing of personal data of jobseekers document and Annex 4 the Applicant's consent to the processing of personal data in the database of jobseekers document.**
- F. **Annex 5 to this Directive is the Information on the Processing of Personal Data of Employees document.**
- G. **Annex 6 to this Directive is Information on the processing of personal data of business partners, contact persons, senders and recipients of shipments and other persons the document.**

Time limits for compliance with the obligation to provide information

- H. The following shall apply with regard to the time limits relating to compliance with the obligation to provide information:
- a) If the Company collects personal data from the data subject, it informs such a subject when obtaining the data;
 - b) If the Company does not collect personal data directly from the data subject, it shall provide this data:
 - a. Within a reasonable period of time once having received the personal data, but no later than one month, taking into account the specific circumstances under which the personal data is processed;
 - b. Where the personal data is to be used for communication with the data subject, at the time of the first communication with that data subject at the latest; or
 - c. If the provision of personal data to another recipient is envisaged, when such personal data is first disclosed at the latest.

3.2 Right of access to personal data

- A. The right of access guarantees the possibility for the data subject to verify which personal data the Company processes.
- B. The data subject has the right to request from the Company access to personal data in accordance with the conditions under Article 15 of the GDPR. The right of access includes, in the first place, the right of the data subject to obtain information as to whether the Company is processing personal data about him or her. Only if the Company processes personal data about the data subject, the data subject has the right to further exercise other rights, namely:
- a) Right to receive information pursuant to Article 15, par. 1 of the GDPR;
 - b) Right to access personal data processed by the Company;
 - c) Right to receive a copy of the personal data being processed.
- C. If the data subject does not explicitly state in their request that they ask for access to personal data or for the provision of a copy of personal data, the Company is entitled to consider a general request under Article 15 of the GDPR as a request to confirm whether personal data is being processed.
- D. When providing information under Article 15, par. 1 of the GDPR, the Company is entitled to use the same way and method of providing information as applicable to the provision of information under Articles 13 and 14 of the GDPR.
- E. The right to receive a copy of personal data under Article 15, par. 3 of the GDPR constitutes a supplementary right of the data subject within the framework of the right of access. By exercising the right to provide information under Article 15, par. 1 of the GDPR, the Company will only provide the data subject with the categories of personal data concerned that it processes about a specific data subject (e.g.: name, age). By exercising their right to receive a copy of personal data under Article 15, par. 3 of the GDPR the data subject applies the right to the provision of a specific "value" of this personal data (e.g.: Joseph, 41). The copy of personal data may be provided in any commonly used electronic form, and one is to reply in writing or electronically at the data subject's request - depending on the manner in which the data subject asks for the copies in question.
- F. The right of access under Article 15 of the GDPR, including any more specific rights that are part of it, must not adversely affect the rights and freedoms of others. "Others" may include, for example, other data subjects or persons other than the data subject making the request.

3.3 Right to rectification

- A. The data subject shall have the right to request the rectification of inaccurate personal data concerning him or her and the right to complete incomplete personal data, even through a supplementary statement. However, the Company as the controller decides whether personal data is incomplete from the perspective of processing purposes. The Company is not obliged to supplement the data subject's personal data at such a subject's request if it does not consider it necessary for the purposes given, as the Company has a general obligation to process only the personal data necessary for those purposes.

3.4 Right to erasure

- A. The right to personal data erasure is mistakenly perceived by the public as an absolute right by which it is possible to arrange for the erasure of all personal data at any time. In fact, the right to erasure applies only in cases defined in Article 17 of the GDPR, which are not of a general or

absolute nature. The data subject has the right to arrange for the erasure of his or her personal data by the Company if he or she proves compliance with any of the above conditions. If the data subject requests the erasure of his or her personal data on the grounds of unlawfulness of its processing, the processing shall only be considered unlawful for the purposes of the right the unlawfulness of which has been decided by the competent court or the Personal Data Protection Authority.

- B. The data subject must provide sufficient reasons for the request for personal data erasure, in particular by referring to a legal provision according to which his or her personal data should be erased (Article 17, par. 1(e) of the GDPR) or by referring to a decision based on which personal data is processed unlawfully by the Company (Article 17, par. 1(d) of the GDPR). The Company is entitled to request additional information from the data subject. The Company is also entitled to refuse to act based on a request for personal data erasure if one of the grounds set out in Article 17, par. 3 of the GDPR applies.

3.5 Right to restrict processing

- A. The data subject shall have the right to request the restriction of the processing in the situations provided for in Article 18 of the GDPR, and the content of these obligations shall be assessed in an adequate manner when reviewing the grounds for personal data erasure explained in par. 3.4 above. If the conditions for the restriction of processing are met, the Company is obliged to restrict such processing within a reasonable period under Article 12 of the GDPR. Within this deadline, the Company will assess whether the request is well-founded.

3.6 Right to data portability

- A. The data subject has the right to request the provision of personal data under Article 20, par. 1 of the GDPR only in relation to the personal data which:
- d) Is processed by automated means (i.e. electronically);
 - e) Is processed on the legal basis of consent or performance of a contract (under Article 6, par. 1(a) or (b) of the GDPR); and
 - f) Is actively provided to the Company by the data subject himself or herself.
- B. The right to portability does not apply to the personal data processed by the Company on legal grounds other than consent or the performance of a contract. The categories of data that do not fall under the right of portability apply in particular to all personal data processed on the basis of a right based on special regulations or the legitimate interests of the Company as explained above.

3.7 Right to object

- A. Data subjects have the right to object, on grounds relating to their particular situation, to their personal data processing by the Company on a legal basis of public or legitimate interests. Upon the receipt of the data subject's request, the Company is obliged to demonstrate to the data subject within the period referred to in Article 12 of the GDPR inevitable legitimate grounds for the processing which override the data subject's interests, rights and freedoms, or such grounds for the establishment, exercise or defence of legal claims.

- B. The data subject has the right to object to personal data processing for direct marketing purposes, in which case the Company is obliged to stop the processing of personal data within the time limit laid down in Article 12 of the GDPR.

3.8 Automated individual decision-making, profiling included

- A. The company shall not conduct any automated individual decision-making, profiling included.

3.9 Exercising data subjects' rights

- A. Data subjects are entitled to exercise their rights under the GDPR vis-à-vis the Company through requests. The processing of requests submitted by data subjects is part of the corporate lawyer - employee's job description; he/she is obliged to proceed in accordance with these Principles and the GDPR.
- B. In the event of any request based on the data subject's rights under the GDPR, the Company shall first identify the data subject in accordance with the provisions of Article 12 of the GDPR. The Company is not obliged to act at the data subject's request unless the identity of the data subject is clearly verified. The persons concerned may contact the Company in person, in writing, electronically or over the phone. However, in each of these cases, the Company is entitled to request the provision of additional information to verify the data subject's identity. This also follows from Article 12, par. 6 of the GDPR, according to which, if the Company has reasonable doubts as to the identity of the natural person making the request, it may request the provision of additional information necessary to confirm such a data subject's identity. In such a case, the Company is entitled, e.g. to refer the data subject to personal verification of their identity on the Company's premises.
- C. The general time limit for data subject's request processing under the Articles 15 to 20 of the GDPR is one month from the receipt of the request given; if, at the time of receipt of the request, the identity of the data subject is not successfully verified, the monthly period only starts to run from the moment of data subject's identity successful verification (hereinafter referred to as the "month period"). The Company is entitled to decide to extend this monthly period by extra two months, taking into account the complexity of the request and the total number of requests received by the Company in that period. Whenever the Company decides to extend the period given, it is obliged to inform the data subject of any such extension and specify the reasons for the delay in the original month period.
- D. If the Company does not take action at the data subject's request, it is obliged to inform the data subject of the reasons for the failure to act and of the possibility of lodging a complaint with the Personal Data Protection Authority or of seeking a judicial remedy within one month as of their request receipt. However, this obligation does not apply to a situation where the Company does not take action at the data subject's request on the grounds of the Company not being able to identify the data subject or of the data subject refusing to provide additional information to verify his or her identity.
- E. For the reasons set out in sentence two of Article 12, par. 5 of the GDPR, the Company is entitled to refuse to act upon request or to request a reasonable fee taking into account the Company's administrative costs connected with the provision of information, notification or the exercise of the requested authorisation. The Company may proceed in this way whenever data subject's

requests are manifestly ill-founded or excessive, in particular because of their repetitive nature. Ill-founded shall be considered data subject's requests:

- a) On the basis of which the data subject unlawfully requests access to confidential or sensitive information, irrespective of his or her intention in relation to that information;
- b) Which are expressly vexatious towards Company's employees or to the Company itself;
- c) Which are vulgar or contain elements of racial, ethnic, gender-related, sexual or religious hatred;
- d) Which are of such a general nature or are so incomprehensible that the Company is unable to assess from the application what right the data subject exercises;
- e) By which the data subject requests information, notification or the basis of the implementation of measures not expressly provided for in Articles 15 to 20 of the GDPR;
- f) Which repeatedly point to the same fact that has already been explained to the data subject several times by the Company and it must be clear to the data subject from the circumstances given that the Company's response had no reason to change;
- g) Which give rise to suspicion of the data subject's intention connected with his or her request to act in the manner that could result in criminal liability or damage to the Company or other persons;
- h) In the case of which the data subject makes video, audio or video recordings of Company employees or the Company itself;
- i) In the case of which the data subject acts aggressively, under the influence of alcohol or narcotic drugs, or endangers the safety of other persons present in the area.

F. The Company shall keep the record of all received data subject's requests concerned and of their handling by the Company in the electronic form at least to the following extent: (i) Date of receipt, (ii) Content of the request, (iii) Method of request handling and (iv) the date of data subject notification.

G. The process of handling requests for exercising data subject's rights is described in the table below:

	Activity	Activity specification	Data protection officer
1	Request receipt	<ul style="list-style-type: none"> Information about the request received is collected and processed by the HR department. Should the request be received elsewhere, it is immediately handed over to the HR department. 	Authorised staff, Legal department
2	Data subject Identification	<ul style="list-style-type: none"> The company verifies and clearly determines the data subject's identity in an appropriate manner, e.g. over the phone via text message or other appropriate means. The Company is obliged to facilitate the exercise of rights and eliminate any ambiguities in cooperation with the data subject. 	Data protection officer, Legal department
3	Checking the legality of requirement	<ul style="list-style-type: none"> The Company will verify whether the GDPR conditions for exercising a specific right have been met. 	Data protection officer, Legal department

4	Personal data identification	<ul style="list-style-type: none"> The Company identifies data subject's personal data it processes and the legal bases for such processing. 	Data protection officer, Legal department
5	Verifying the existence of legitimate grounds for personal data processing	<ul style="list-style-type: none"> In the event of a legitimate complaint against the processing, the Company will verify whether it is necessary to continue processing the data subject's personal data. This may be the case if: <ul style="list-style-type: none"> There are legitimate grounds for the processing which override the data subject's interests, rights and freedoms; or Such processing is necessary for performance. 	Data protection officer, Legal department

4 Impact assessment and prior consultation

A. The Company conducted an analysis of the obligation of impact assessment and prior consultation; these obligations do not arise in connection with the processing operations conducted by the Company.

5 Personal data security

5.1 Adequacy of security measures

A. The Company shall ensure an adequate level of protection at any time in accordance with the GDPR with regard to:

- Latest knowledge;
- Costs of measure implementation;
- Nature, scope, context and purposes of the processing;
- Risks of varying likelihood and severity for natural persons' rights and freedoms.

B. To ensure personal data security and integrity, the Company has implemented some or all of the following measures:

- Personal data pseudonymisation and encryption;
- Ability to ensure permanent confidentiality, integrity, availability and resilience of processing systems and services;
- Ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;
- Process of regular testing, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing.

C. The company also ensures the protection of personal data through regular training of the employees who are authorised to access personal data as per their job description. The training shall be conducted at least once a year.

D. The Company performs its activities for the purpose of identifying, evaluating and managing information security risks. The existing and new hardware is configured professionally. The Company shall ensure the safe use of portable storage devices (USB, CD). The Company assigns user accounts to employees so that they only have access to the information/equipment/data they need to perform their work. The company obliges its employees

to change access passwords to computers and programs on a regular basis. The Company ensures the detection of any unauthorised access to such computers and programs.

- E. Authorised persons are obliged to process personal data in such a way that unauthorised or accidental access to, alteration, destruction or loss of personal data, unauthorised transfers, other unauthorised processing as well as other misuse of personal data cannot take place.
- F. Documents and digital recording media containing personal data shall be secured in a lockable place in the Company, or in other places where their protection can be ensured. A record of employees' access to personal data is kept, indicating at least what personal data and for what reason was made available.
- G. Data containing personal data stored on the Company's or employees' servers is secured against free access by unauthorised persons, from the alteration, destruction, loss, unauthorised processing, as well as other misuse of personal data, in particular by using individual user passwords, encryption, backup, etc.
- H. The Company employees are not entitled to upload personal data to any portable computer or any portable data carrier that may be taken from the Company's premises. An exception is granted to authorised persons if the personal data is encrypted or other technical or security measures have been introduced.
- I. The Company employees with access to personal data are obliged to maintain confidentiality of personal data and of the security measures taken to protect personal data. Authorised persons are obliged to handle personal data only for the purpose of fulfilling their obligations and in accordance with the obligations laid down by the relevant legislation, this Directive and the Company's instructions.
- J. The Company keeps records of personal data processing in accordance with the GDPR for each processing of personal data separately according to its purpose (Annex 1 to this Directive – Records of Controller Activity Processing).
- K. The Company as well as the authorised person will arrange for the supervision of the entry of personal data into the respective systems and its processing and will keep records of personal data, including the data on its disclosure or provision to third parties. The Company also keeps records of the authorised persons who are allowed to process personal data, including the form, scope and reason why personal data is processed by these persons.

5.2 Notification of personal data breaches

- A. The Company shall notify of a personal data breach within 72 hours from the verification of whether a personal data breach has occurred and what risks it may pose to natural persons' rights and freedoms. The Company is obliged to conduct such verification in accordance with the previous sentence without delay after finding that a personal data breach may have occurred.
- B. The Company shall notify a personal data breach under Article 33 of the GDPR by means of a special form published on the website of the Personal Data Protection Authority of the Slovak Republic or via the form set out in **Annex 7 of this Directive**.

6 Other entities involved in personal data processing

6.1 Personal data provision

- A. When the Company performs its activities, personal data is provided to other entities by the Company as a controller. Given that neither the GDPR nor the Personal Data Protection Act expressly makes the provision of personal data to another entity subject to the data subject's consent, the provision of personal data is a processing operation that can take place on any legal basis permitted by the GDPR.
- B. In some cases, the Company is obliged to provide personal data to other entities under special regulations. The personal data processed by the Company may be accessed by the Personal Data Protection Authority, law enforcement authorities, tax authorities and other entities.

6.2 Use of processors

- A. The Company may use processors who process personal data on its behalf to process personal data. The use of processors is not subject to the data subject's consent. If the processing is to be performed on behalf of the Company, the Company shall use only the processors providing sufficient guarantees that appropriate technical and organisational measures will be taken so that the processing meets the requirements of the GDPR and to ensure the protection of data subjects' rights.
- B. **Annex 8 to this Directive contains the list of such processors.**

7 Data Protection Officer (DPO)

- A. The Company has performed an analysis of the obligation to appoint a DPO and the analysis results in the fact that it does not have such an obligation.

8 Personal data destruction

- A. The Company regularly disposes of personal data the purpose of processing of which no longer exists. The deletion of outdated and unnecessary personal data is carried out by designated Company employees once a year on a regular basis. The disposal shall be performed in a technically secure manner in such a way as to eliminate the risk of data misuse. Paper data carriers shall be shredded and electronic media shall be deleted to ensure that personal data cannot be restored.

9 Final Provisions

- A. This Directive shall be available to all employees of the employer as follows: posted on Alfresco.
B. This Directive also contains annexes.

Annex 1 – Records of controller processing activities (unpublished, available for consultation at Legal Department of cargo-partner SR, s.r.o.; for internal purposes only)

Annex 2 – Matrix of employees authorised to process personal data (unpublished, available for consultation at Legal Department of cargo-partner SR, s.r.o.; for internal purposes only)

Annex 3 – Information on job seekers' personal data processing

Annex 4 – Applicant's consent to the processing of personal data in job seekers database – SPECIMEN

Annex 5 – Information on employees' personal data processing

Annex 6 – Information on business partners, contact persons, shipment senders and recipients and other persons’ personal data processing

Annex 7 – Notification of personal data security breach – SPECIMEN

Annex 8 – List of processors (unpublished, available for consultation at Legal Department of cargo-partner SR, s.r.o.; for internal purposes only)

10 Glossary of terms

Abbreviation	Meaning
GDPR	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, repealing Directive 95/46/EC
Law	Act No. 18/2018 Coll. on personal data protection and on amendments and supplements to certain acts, as amended
Authority	Personal Data Protection Authority of the Slovak Republic
Directive	Internal personal data processing directive at issue
Personal data	Any information relating to an identified or identifiable natural person (hereinafter referred to as the " Data Subject "); the 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, on-line identifier or to one or more factors specific for the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person in question.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise ways of making available, alignment or combination, restriction, erasure or destruction, whether or not by automated means.
Information system	Any organised set of personal data accessible according to specified criteria, whether centralised, decentralised or distributed on a functional or geographical basis.
Controller	Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of personal data processing.
Processor	Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Recipient	Natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether or not a third party. However, public authorities which may receive personal data in the context of a specific inquiry in accordance with Union or Member State law shall not be deemed recipients; the processing of such data by those public authorities shall be conducted in accordance with the applicable data protection rules, depending on the purposes of such processing.
Third party	Natural or legal person, public authority, agency or body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process personal data.
Data subject’s consent	Any freely given, specific, informed and unambiguous indication of data subject’s will by which he or she, by a statement or by a clear affirmative act, signifies their consent to the processing of the personal data relating to him or her.
Breach of personal data protection	Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

11 History of Changes

Date	Name	Description
27/03/2024	Lucia Karlíková	Initial document, that follows the original 2018 internal documentation, which was not published as an internal directive in Alfresco, but made available on the website of cargo-partner SR, s.r.o. DCR-1676
29/11/2024	Diana Federicova	Updating of the Directive in relation to the conflict of interest questionnaire (changes to Annex 1, Annex 5, new proportionality test /prevention and avoidance of conflict of interest/, proportionality test - security of information systems - modified). Updating of the Directive also in connection with the new Intracompany Agreement (ICA) on the processing of personal data (updated Annex 1 and Annex 8 of the Directive). DCR-1913

12 Annex 3 – INFORMATION ON JOB SEEKERS' PERSONAL DATA PROCESSING in cargo-partner SR, s.r.o.

Under 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 the “**GDPR**”)

1. Controller's identification data

Within the meaning of the GDPR, the controller is the company:

cargo-partner SR, s.r.o. registered office: Kopčianska 92, 851 01 Bratislava – Petržalka City District, Company ID: 31 358 152, entered in the Business Register maintained by the Bratislava III City Court, Section Sro, Entry No.: 5741/B (hereinafter referred to as the “**Company**”).

In this document, as a data subject who is not an employee of the Company, you will find all the elements required by Art. 13 of the GDPR as well as other necessary information regarding the processing of your personal data by our Company.

2. Personal data we process

Anyone interested in working for the Company can apply for employment through the Profesia.sk job portal, the company's online portal (cargo-partner website), via social networks (e.g. LinkedIn), or by sending a written request to the Company's address by post, email or delivery in person. The categories of personal data processed include, in particular, your so-called main data in the scope of title, forename, surname, address of permanent residence, address of temporary residence, age, gender, all data and other records included in the official education document, signature, contact details (in particular telephone number and e-mail), information given in your CV, language skills, experience, courses completed (name, period of validity, publisher, country), skills (name, level), expected salary, expected focus, expected place of work and other data included in the CV, motivation letter and staff questionnaire for the purpose of registering job seekers; where appropriate, other data collected during the selection process, Thomas test and personal questionnaire data, manuscript or signature included.

In case of attending a personal job interview at the company headquarters or on any other premises where the CCTV camera system is located, we may also collect videos of your person.

3. How we collect your personal data

We process personal data that you voluntarily provide to us during the selection process. You provide us with personal data through the professional portal Profesia.sk, the company's online portal (website cargo-partner), social networks (e.g. LinkedIn), by sending a job application by post, e-mail or delivery in person, or during communication during the recruiting process.

Video recordings are automatically recorded by the camera system.

Your personal data is necessary for the execution of the selection process and you cannot participate in this process without providing the data.

4. Purposes and legal basis of processing

We process your personal data solely for the purposes set out in this Information and on the basis of the legal grounds for processing determined by the applicable legislation relating to personal data protection: Your personal data is processed for the purpose of carrying out the selection process, so that, upon your request, we make efforts before concluding an individual employment contract or other contract with similar effects and in order to meet the legal conditions for filling the position you are applying for (including references from your previous employers and creating your psychological profile by using the data you provided in the Thomas test, personal questionnaire and your manuscript).

The legal basis for this processing is Art. 6, par. 1(b) of the GDPR – the processing is necessary so that all the measures requested by the data subject are taken prior to entering into a contract.

Your data may be used to verify compliance with legal obligations related to the recruitment process.

The legal basis for this processing is Art. 6, par. 1(c) of the GDPR – processing is necessary for compliance with the controller’s legal obligation.

Your data may be used to defend the Company against complaints and claims brought by bidders.

The legal basis for this processing is Art. 6, par. 1(f) of the GDPR – processing is necessary for the purposes of legitimate interests pursued by the controller – defence against anti-discrimination actions by job seekers.

Video recordings recorded automatically by CCTV camera system are used for the purpose of protecting the company’s property and for the purpose of ensuring the safety and health of employees and other persons residing lawfully on the company’s premises.

The legal basis for this processing is Art. 6, par. 1(f) of the GDPR – processing is necessary for the purposes of the legitimate interests pursued by the controller.

We may process your personal data in the candidate database for the future selection procedure that you may be interested in only if you give your explicit consent to the purpose given. If you wish to be contacted if a suitable job is vacant, your consent to the processing of personal data (following a negative assessment of your earlier job application) is necessary.

The legal basis for this processing is Article 6, par. 1(a) of the GDPR – the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Data is processed for reporting and statistics purposes. This processing is anonymous, so no identification of individual personal data is possible.

The legal basis for this processing is Art. 6, par. 1(f) of the GDPR – processing is necessary for the purposes of the legitimate interests pursued by the controller.

You have the right to know the purpose for which we process your personal data. We will inform you before we start processing your personal data for any other purpose.

5. Processing time

We will process your personal data for the entire duration of the selection process and for the following two years if you have given us your consent to process such data in the job seeker database.

We will process your personal data for as long as we need to be able to demonstrate non-discrimination, i.e. 3 years after the completion of the selection process.

Video recordings of your person created by the CCTV camera system will be processed for a period of 30 days from their creation and after this period they will be automatically deleted.

6. Personal data recipients

The recipients of your personal data may be the management of the company, selected service processors, authorised employees of all cargo-partner group companies and nippon express, competent state authorities, if desired. All service processors entrusted with the processing of your personal data are selected carefully so as to ensure the processing of personal data while maintaining your data confidentiality and an adequate level of security.

If the data is disclosed to another recipient (private natural or legal person, public authority or any other body) not mentioned above, we will inform you in writing, unless such data transfer is expressly provided for in the legal regulations of the European Union or on the national level.

7. Personal data protection

In order to ensure the confidentiality, integrity and availability of data subjects' personal data, the Company uses modern IT security systems. The Company maintains appropriate technical and organizational security measures against unlawful or unauthorised processing of personal data and against accidental loss or damage of such data. Access to personal data shall be granted only to those who need it in order to fulfil their professional obligations and who are bound by the legal or contractual obligation of confidentiality.

8. Data subject's rights

You have the following rights regarding the processing of your personal data:

Right of access to your personal data: You have the right to be informed about what personal data is collected and stored by our company as well as the purposes of their processing and their recipients.

Right to rectification of your personal data, completion of incomplete personal data and the right to personal data erasure: You have the right to request the rectification of inaccurate, incomplete or outdated personal data and the erasure of your personal data, for example, if the processing is not necessary or is unlawful, if you have withdrawn your consent to the processing of personal data you previously granted. The personal data processed based on legal regulations cannot be erased.

Right to restrict processing of your personal data: In the cases provided for by the GDPR, you can request the restriction of the processing of your personal data. For example, if the accuracy of the data is contested, you may require that your data be processed only with your consent or for the purpose of asserting, exercising or defending legal claims, or in order to protect your right to privacy or the right to privacy of another natural or legal person, or for reasons of important public interests.

Right to data portability: You have the right to ask us to send you, or, if technically possible, to a third party designated by you, a copy of your data in a structured and readable format.

Right to object to the processing of your personal data: You may exercise this right in relation to personal data if it is processed on the basis of the controller's legitimate interests, public interest or if it is used for profiling.

Right to withdraw consent regarding the processing of your personal data in the job seeker database: The consent may be revoked at any time and your personal data will be deleted from our database of job seekers as soon as possible, but no later than in 30 days.

9. Exercising your rights

If you have any questions about the processing of your personal data or if you wish to send us a request, or if you wish to exercise any of your rights regarding the processing of personal data, please contact us at the following email address: **integrity.sk@cargo-partner.com**, or directly at the address of our company cargo-partner SR, s.r.o., Kopčianska 92, 851 01 Bratislava – Petržalka City District.

If you believe that the processing of your personal data is in conflict with the GDPR, you can lodge a complaint with the **Personal Data Protection Authority of the Slovak Republic**, Hraničná 4826/12, 820 07 Bratislava. The given authority shall be competent to deal with any complaints relating to personal data processing.

Thank you for entrusting us with your personal data and for taking the necessary time for reading the information about how it is processed. Do not hesitate to contact us if you have any questions regarding your personal data processing.

Effective from: 27/03/2024.

13 Annex 4 – APPLICANT’S CONSENT TO THE PROCESSING OF PERSONAL DATA IN JOB SEEKERS DATABASE

I, the undersigned:

Forename and surname:

Email address:

Telephone Number:

Hereby grant **cargo-partner SR, s.r.o.**, Company ID: 31 358 152, registered office: Kopčianska 92, 851 01 Bratislava – Petržalka City District, entered in the Business in the Buisness Register of the Bratislava III City Court, Section Sro, Entry No. 5741/B (hereinafter referred to as the “**Company**”) **consent to the processing of my personal data** for the purpose of keeping it in the Company’s database of applicants in case of a new or vacant position being created in the Company.

Scope of personal data

I give my voluntary consent to the processing of personal data included in the personal questionnaire, the data contained in my CV sent to the Company and the data obtained by the Company from publicly available sources (e.g. from the Business Register or professional social networks such as LinkedIn), in particular data on my educational background, qualifications and experience.

Time of personal data processing

I grant this consent **for the period of 2 (two) years from the date the selection process for filling the job position is completed.**

I declare that the personal data provided is true and up-to-date and have been provided freely, and I have been informed about the processing of personal data in accordance with Art. 13 of the GDPR.

What are your rights?

You can withdraw this consent **at any time** at the address of cargo-partner SR, s.r.o., Kopčianska 92, 851 01 Bratislava or electronically by writing to **integrity.sk@cargo-partner.com**. The withdrawal of the consent does not affect the lawfulness of personal data processing on the basis of the consent before its withdrawal. Further information on personal data processing and your related rights can be found on the Company’s website in the “Download” section at: <https://www.cargo-partner.com/contact/Europe/Slovakia> OR attached to this consent.

By signing this document, I confirm that I am familiar with the “Information on job seekers’ personal data processing in cargo-partner SR, s.r.o.”.

In (place) _____ , on (date) _____

Signature

14 Annex 5 – INFORMATION ON EMPLOYEES' PERSONAL DATA PROCESSING

Under the Articles 13 and 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 the „GDPR“)

In the context of your employment relationship with our Company, it will be necessary for us to process certain data that is considered personal within the meaning of the GDPR, subject to the protection provided for in the above Regulation.

We would like to provide you with information on how we will process personal data and what are your rights as a data subject.

Controller's identification data

Within the meaning of the GDPR, the following company acts as a controller:

cargo-partner SR, s.r.o.

Registered office: Kopčianska 92, 851 01 Bratislava – Petržalka City District

Company ID: 31 358 152

entered in the Business Register maintained by the Bratislava III City Court. Part: Sro, Entry No.: 5741/B

(hereinafter referred to as “we” or “our company”).

Purposes and legal bases for personal data processing

The provision of the absolute majority of your personal data that we process is a **legal requirement** or it is **necessary for the performance of a contract** you enter into with our company. Without providing this data, it will not be possible to carry out the employment relationship.

At the same time, some of your personal data will also need to be processed for the purposes of **legitimate interests** pursued by our company or by a third party.

Meeting legal obligations

Our company has legal obligations that it is to perform, especially in the field of labour law, taxes, health insurance, social security and legislation related to the line of our business.

Such legislation is, for example, the Labour Code, Act No. 461/2003 Coll. on social insurance; Act No. 595/2003 on income tax, Act No. 563/2009 on tax administration, Act No. 580/2004 Coll. on health insurance; Act No. 43/2004 on pension scheme contributions, Act No. 283/2002 Coll. on travel expense reimbursement, Act No. 5/2004 Coll. on employment services, Act No. 124/2006 Coll. on occupational health and safety, Act No. 355/2007 Coll. on the protection, promotion and development of public health, Act No. 54/2019 Coll. on the protection of whistle-blowers reporting anti-social activities, the GDPR as amended as well as other legal regulations.

We process personal data to the extent that to which it is necessary for the fulfilment of specific legal obligations with the scope, duration and purpose of processing being laid down in the aforementioned legal regulations. In this context, we may also process special categories of personal data – in particular data on reduced working capacity, disability, alcohol consumption, the use of narcotic drugs and psychotropic substances, etc. (if required by law).

The personal data processed in this way may include the data of your family members (if you provide them, e.g. in connection with compliance with tax obligations). According to Art. 14 of the GDPR, we add that this personal data of family members falls within the general (basic) category of personal data and you provide it to us as our employee.

Entering into contract and contract performance

The content of our employment relationship consists of our mutual rights and obligations governed by the employment contract or agreement on work performed outside the employment relationship, and our internal regulations. Therefore, we also process your personal data for the purposes of entering into and performing such an employment contract or agreement.

For this purpose, mostly basic personal data, in particular the person's identification data, contact details (including private telephone number and private e-mail address), information about your education, employment background, your qualifications, the data you provided in your curriculum vitae, your job description, job tasks, pay, attendance, work results, evaluation of the employee's work including his/her personal prerequisites/properties, training, existence and reason of the obstacles to work on the part of the employee (including the health data listed there), assessments, information related to the entrusted work equipment /keys/access cards and rights, inventory results, duration of holidays and sick leaves, maternity leave, parental leave, business trips, third party liability insurance, facts related to possible violation of work discipline, content of employment contracts, agreements, their appendices, work performance reviews, documents relating to the termination of the employment relationship, if you have been assigned a business car – its state plate number, data resulting from its use, fuel billing, or, in the case of the use of your private vehicle also the state plate number, a copy of the third party insurance premium and the technical certificate; in the case of foreigners, the data contained in the residence permit; where appropriate, other information arising from the course of the employment relationship; but also special categories of personal data, is commonly processed and so are the records of accidents at work, pregnancy data for the purposes of protection provided to pregnant women, etc.

The data you provide in the Thomas test and in the personal questionnaire, including your manuscript, is used to create your psychological profile (to verify the match between your psychological profile and the profile required for the job you applied for) based on the efforts you have made to enter into and perform such an employment contract.

If you also enter into another contract/agreement with our company (e.g. an agreement on the use of a company//private vehicle, an agreement on material liability, an agreement on damages, an agreement on work performed outside employment relationship, etc.), we will also process your personal data for the purpose of entering into and performing such a contract/agreement.

Legitimate interest

If we process personal data for the purpose of implementing or protecting our legitimate interest, we may process personal data to the extent necessary even without your consent being given. The legitimate interests for which we process your personal data in this way are:

Interest in the protection of our company's and employees' assets and in ensuring the safety and health of our employees and other persons lawfully staying on our premises, as well as for the mutual recognition of employees among themselves, especially when moving in the areas requiring increased security measures;

We may process the necessary identification data and your profile photo to issue an access card proving your contractual relationship with our company and monitor access to our premises;

Through our CCTV camera system, we can monitor people entering the site, a building, building circulation areas (excluding offices and social facilities);

We can monitor staff entry into a building through the building security system accessible on the basis of employee input codes;

We may process your forename, surname and signature in the written records of warehouse entries, thus monitoring the entries into our warehouses.

Interest of our company and of third parties (companies within our cargo-partner and nippon express group) **in the management and efficient organisation of our company, the performance of reporting and administrative activities within the group and other internal administrative purposes;**

We may process your personal data in the form of tables, organigrams, mailing lists, organisational charts, when budgeting, and we can share it with other companies within the group;

In order to facilitate communication within the group, employee cooperation, creation of international work teams, organisation of business and employee events, etc., we may process your personal data in the company lists of employees' contact details, your profile picture included,

As the content of your corporate e-mail communication is part of our company's business correspondence, we may also access and forward emails delivered to your corporate email address to other group employees in order to avoid damage resulting from unfinished tasks in the event of your incapacity for work, vacation or employment termination.

Interest in ensuring the confidentiality of personal data, commercially sensitive information and information on our clients, interest in ensuring compliance with the rules and processes relating to personal data protection included.

Interest in ensuring network and information security;

For the purposes of (c) and (d), we may, for example, process:

Your login data and passwords to our systems, records of your instructions, training, logs and records of access to our systems, your activity on the systems, in particular for the purpose of detecting unwanted activity, possible data leakage or data corruption, loss or destruction, your telephone number for the purpose of multi-factor authentication to prevent unauthorized access to our electronic communication networks (systems), to the extent necessary, to monitor or restrict the use of the Internet on business devices, to investigate security incidents, etc.

Interest in exercising or protecting our rights in various administrative, arbitration, criminal, judicial or enforcement proceedings, as well as in extrajudicial proceedings and negotiations;

We process personal data necessary for such exercising or protection of rights, including those originally collected for other, prior processing purposes, as well as for obtaining information and supporting documents, and verifying such information and documents for these purposes. This data may, in exceptional cases, also include the content of employees' work email boxes.

Interest in promoting our company and various forms of communication both externally and internally;

We may process your profile photo in order to facilitate communication with the external environment (customers/suppliers/state authorities) and personalised access to our clients; the publication of one's profile picture is particularly important in the case of managing employees;

To personalise e-mail communication both internally and externally, we can use your profile photo as part of a uniform standard, along with other contact details in the unified signature of email messages sent from employees' work e-mail accounts;

We may process photographs and videos from various events, educational events and events organised or co-organised by our company for the purpose of informing on our activities, the activities of our employees at various events organised by our company at or outside the workplace, as well as their regular work activities, building public, business partners and potential employees' awareness of our activities and our employees' satisfaction, promoting our company and its social policy, promoting our team spirit and increasing the attractiveness of our company from the perspective of potential employees and business partners by producing such photographs and videos and publishing them on various communication channels (website, social networks, Intranet, etc.) and to that related photo archiving and video documentation to the extent required. Photographs and/or videos will always be posted to the extent necessary for meeting the purpose given and will not interfere in any way with the employees' privacy or dignity or otherwise violate their personality protection right. Failure to provide your personal data (refusal to be photographed) will have no negative consequences, except for limiting your participation in certain activities during events.

Interest in employees' proper education and personal development;

We may process course and learning data, operate your e-learning account, test and assess your personality potential, language proficiency and managerial skills, both physically and by electronic means, including evaluation of results by electronic means.

Our company uses this information to ensure targeted further training of employees as well as optimal filling of key positions in the Company. Such test results, however, will not have any negative impact on the employee.

Interest in OSHA task performance and in first aid provision:

We may process data about completed OSHA and first aid courses (e.g. your name, surname, photo and contact number or email), either by posting data on the Company board or via electronic means.

Interest in Preventing and Avoiding Conflicts of Interest

We may process your personal data and the personal data of individuals close to you, aiming to minimize the risks associated with promoting your personal interests and to ensure that decisions are made in the best interest of our company and the cargo-partner and nippon express group as a whole.

Personal interests include financial, familial, kinship, or other relationships with customers, suppliers, or competitors that could compromise your judgment, decision-making, or actions within our company. Such personal interests may affect the quality, integrity, ethics, fairness, or reliability of outcomes. They may harm the reputation of the operator and the business partner, impact financial results, lead to damages, or result in breaches of legal regulations.

The processing of personal data for this purpose involves, in particular: (i) determining whether you are in a conflict of interest, for example, by having a familial relationship, ownership connection (if the entity is a legal person), or other personal interest in the outcome of a service or performance concerning a business partner or competitor; (ii) identifying whether you are engaged in other gainful activities; (iii) identifying whether your family members and other close individuals perform activities for an entity within the cargo-partner and nippon express group or for a competitor; (iv) implementing procedures and measures designed to prevent conflicts of interest from arising; and (v) conducting control measures aimed at verifying the functionality and adherence to the measures adopted to prevent and avoid conflicts of interest.

Under Article 21 of the GDPR, you have **the right to object** to the processing of your personal data on the basis of the controller's legitimate interests on grounds relating to your particular situation. This right may be exercised at the employer in the manner specified in In Article 5 below. Should there be any photos or videos of you taken at events, you can also object directly there.

Employee's consent

With your prior consent, we may also process your personal data for other purposes.

You are not obliged to grant your consent to the processing of personal data for any purpose, it is your voluntary decision and you can withdraw your consent at any time; the withdrawal of such consent does not affect the lawfulness of personal data processing prior to consent withdrawal.

Who has access to your personal data

For the purposes of fulfilling legal obligations, it is necessary that we disclose or give access to your personal data to third parties (recipients); these are mostly individual public administration authorities (e.g. tax office, Social Security Insurance Company, health insurance companies, inspection bodies, etc.).

In order to provide employee benefits, it is also necessary to provide your personal data to selected entities providing relevant services.

When performing our activities, we can also use the services of other entities where necessary, e.g. for the management of payroll and human resources agenda, education, catering for employees, ensuring occupational health and safety and fire protection, administration of attendance-recording software solution, administration of the CCTV camera system, building protection who process personal data on behalf of our company as our processors.

These entities (in the GDPR designated as processors) are selected carefully so as to ensure the processing of personal data while maintaining their confidentiality and an adequate level of security. Contracts with processors contain provisions that ensure the protection of your personal data. Moreover, the processors are subject to regular review to ensure compliance of the processing of personal data with these provisions, as well as with the GDPR provisions. The processors are provided with personal data only to the extent necessary for the individual purposes of such data processing.

Our company is a member of the global cargo-partner and nippon express group. Your personal data may be transferred to companies belonging to the cargo-partner and nippon express group both within and outside the European Union for the purpose of processing (i) for the promotion of our company and various forms of communication both externally and internally, (ii) for internal administrative purposes, and (iii) for the purpose of preventing and avoiding conflicts of interest.

As stated above, the legal basis for this data sharing is a legitimate interest on the part of the controller and other group companies. In the case of non-EU companies, we will ensure adequate data protection, which means that the protection of personal data is in line with the level of protection applied within the EU/EEA.

As your employer, we are, at the same time, authorised (under Section 78, par. 3 of Act No. 18/2018 Coll. on the personal data protection as amended) **to provide your personal data to third parties if necessary in connection with the performance of your professional duties**; the data will be provided in the following scope: degree, forename, surname, job title, employee's personal number or employee number, professional department, place of work, telephone number, fax number, e-mail address to the workplace and employer's identification data. The provision or disclosure of personal data will have no negative impact on others' respect for you, your dignity or security. We are also entitled to **disclose** personal data to the above extent. Your personal data will not be subject to automated decision-making or profiling.

Period for which the personal data will be kept

Your personal data will be kept for as long as necessary to achieve the purpose and unless this is contrary to the controller's obligation to delete it (e.g. the obligation to retain the data on the basis of tax and accounting regulations, the Social Insurance Act, the Health Insurance Act).

Personal data required for human resources management (employee's personal file) is kept for 70 years from the employee's birth. Your payroll records (employee payroll card) are kept for 50 years after the termination of the employment relationship. These retention periods are recommended to prove your rights in the future, especially when exercising the right to old-age pension. The retention periods of all types of documents are stipulated in our company's Registry Plan.

Recordings from the camera system located on the employer's premises shall be kept for no more than 30 days from the date of their production. If a record is used in criminal or other proceedings to prove the circumstances of a damage, crime, offence etc., we keep those for as long as necessary for the purpose given.

Your rights related to personal data processing

Your rights under the GDPR depend, to a large extent, on the legal basis for personal data processing. This means that when processing your personal data necessary for legal purposes or for the performance of an employment contract, your rights are limited in a certain way (e.g. we will not be able to exercise your right to delete personal data because we would breach the law).

Under the GDPR, you have the following rights:

You can ask us to confirm that we process your personal data. At the same time, you have the right to ask us for a copy of your personal data that we process. Please note that in case of repeated requests to provide these copies, we have the right to charge an administrative fee. **(Right of access)** This right also includes our obligation to provide you with the information contained in this instruction, as well as the rights set out below.

You may request the rectification of your personal data if your personal data that we process is incorrect or outdated. If you exercise this right, we are obliged to correct your incorrect or incomplete personal data as soon as possible **(Right to rectification)**. Please note that in the case of an employment relationship, you are, under the Labour Code, obliged to notify your employer without delay of any change in your personal data;

We are obliged to delete your personal data if the purpose of the processing has expired, the period for which you provided such data to us has expired, or your personal data is not necessary to achieve the purpose for which it was provided. Our obligation to erase your personal data is also related to your right to withdraw consent to personal data processing (in the event of your consent to personal data processing withdrawal, this revocation will not affect the lawfulness of the processing prior to consent withdrawal); Please note that even if you request the erasure of your personal data, the applicable law may oblige us to retain some of your personal data (e.g. tax regulations).

We will then mark your personal data to ensure that it is not used for any purpose other than the one in which it is stored. **(Right to erasure and Right to withdraw consent)**.

You may also request the restriction of processing in cases where (i) you have challenged the correctness of the data in question for the period during which we verify such data correctness, or (ii) the processing is unlawful, but you do not want to delete the data, or (iii) the data is no longer necessary for us for the original purpose, but you need it to prove, exercise or defend legal grounds, or (iv) when your objection to processing is being reviewed. "Restriction" means that, with the exception of retaining, your personal data may only be processed with your consent and only for the establishment, exercise or defence of legal claims, for the

protection of the rights of another natural or legal person or for reasons of public interest of the EU or of an EU Member State. If the restriction is lifted, it is our duty to inform you in advance (**Right to restrict processing**);

You may ask our company to send you, or, if technically possible, to a third party appointed by you, a copy of your data processed on the basis of consent or on the basis of a contract in a structured and readable format (**Right to data portability**);

You can object to the processing of your personal data even if we process your personal data on the basis of a legitimate interest, and if, at the same time, your rights and freedoms outweigh our or a third party's legitimate interest (**Right to object**);

If you believe that the processing of your personal data is in conflict with the GDPR, you can lodge a complaint with the Personal Data Protection Authority of the Slovak Republic, Hraničná 4826/12, 820 07 Bratislava. The given authority shall be competent to deal with any complaints relating to personal data processing. (**Right to lodge a complaint**).

Exercising rights

If you have any questions about your personal data processing or if you wish to send us a request or wish to exercise any of your rights related to personal data processing, please contact us at the following local e-mail address: **integrity.sk@cargo-partner.com**; or directly at our company's address: **cargo-partner SR, s.r.o., Kopčianska 92, 851 01 Bratislava – mestská časť Petržalka**.

We will try to resolve such a request as soon as possible, yet no later than in one month. If we need further information from you or have problems resolving your request, we will immediately inform you that we need more time to adequately analyse your request.

If you believe that we have not resolved all your requests, or you are not satisfied with our replies, you may lodge a complaint with the Personal Data Protection Authority.

Your personal data security

We consider the security of your personal data to be our top priority. We assure you that all the information you provide to us is secure and is considered strictly confidential. We use standard procedures to maintain the confidentiality, integrity and availability of personal data, e.g. by using access controls. All personal data provided to us is secured through standard processes. We strive to regularly update our security measures to apply new procedures and processes.

Further information

If this information on the processing of employees' personal data is updated or if we would like to process your personal data for other purposes, we will inform you in an appropriate manner. This information on the processing of employees' personal data is also available at Alfresco. You are obliged to make yourself familiar with possible revisions of the document, which you will be kept informed of.

Effective from: 27/03/2024.

15 Annex 6 – INFORMATION ON BUSINESS PARTNERS, CONTACT PERSONS, SHIPMENT SENDERS AND RECIPIENTS AND OTHER PERSONS' PERSONAL DATA PROCESSING,

Under the Articles 13 and 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 the „GDPR“)

This document provides you with information on your personal data processing by **cargo-partner SR, s.r.o.**, as well as on your rights related to such processing. **Cargo-partner SR, s.r.o.** acts as a controller when processing your personal data, i.e. an entity that determines the purposes and means of processing and decides on the processing of your personal data for the purposes listed below.

Contact details:

cargo-partner SR, s.r.o.

Registered office: Kopčianska 92, 851 01 Bratislava – Petržalka City District

Company ID: 31 358 152

entered in the Business Register maintained by the Bratislava III City Court, Part. SRO, Entry No.: 5741/B

Telephone: +421 (0)2 68242 300

Fax No.: +421 (0)2 68242 222

(hereinafter referred to as the “**Company**” or “**we**”)

What data we process

We process the following personal data:

Identification data, which mostly means: degree, forename and surname, Company ID and Tax ID, if you are an entrepreneur, and your position in the organisation if you represent a legal entity;

Contact details, which means personal data that enables us to contact you, in particular e-mail address, telephone number, delivery address, takeover address, billing address;

Details of the services ordered, which are mostly: details of the shipments you or your company have ordered with us, the payment method including the payment account number, and the details of complaints;

Data necessary for customs clearance, if you have authorised us to represent us, your national identification number included;

Data related to your visit to our establishment, in particular recordings from CCTV camera systems at branches and recording of entries to storage areas;

Data related to your visit of an event organised by our company, in particular photos and videos.

Why do we process personal data and what entitles us to do so?

In the context of our activities, we process personal data **for different purposes and based on different legal grounds**:

On the basis of contract performance (Article 6, par. 1(b) of the GDPR);

Based on our legitimate interest (Art. 6, par. 1(f) of the GDPR);

For the performance of our legal obligation (Article 6, par. 1(c) of the GDPR);

Based on your consent (Article 6, par. 1(a) of the GDPR).

What processing we may conduct without your consent depends on the purpose for which the processing will be conducted and in what your position towards us is – whether you have a contract with us, you have ordered a service or there is no contractual relationship between you and our company at a given time. We may also process your data if you are the consignor or consignee and you ask us to have your shipment arranged by us, if you communicate with us, if you visit our premises or an event organised by our company. When processing personal data, our company does not conduct any automated decision-making or profiling.

Purposes of personal data processing

If you order us to ship a consignment for you or enter into a contract with us

If you order us to ship a consignment for you or enter into a service contract or other contract with us, we perform the following processing:

Processing based on performance of a contract

If you, as a natural person, order us to ship a consignment for you, we process your personal data for the purpose of **transporting and tracking the shipment**. In the case of any other agreement entered into to fulfil the given contract (e.g. customs clearance mandate agreement), **we need your identification and contact details, details of your orders, and data necessary for customs clearance**.

If you order transport of a shipment as an employee of a legal entity, we process your identification and contact details and the data of the ordered services **for the purpose of transporting and tracking the shipment** the case of any other agreement entered into to fulfil the the given contract under Section 78, par. 3 of Act No. 18/2018 Coll. on personal data protection and on amendments and supplements to certain acts ("**Personal Data Protection Act**").

The fact that we use this data for the purpose of transporting and tracking a shipment or performing a contract means that we will mainly use it:

To communicate with you about the shipment being transported, for example, to send you a confirmation of its delivery;

For the purposes of payment for the transport or other service or for the purposes of service rendering; in this context, we may also disclose your data to our shipping partners as described in the "Who processes your personal data and to whom we disclose it?" section;

In connection with complaints;

In relation to other of your requests/inquires.

Processing on the basis of legitimate interests

If you order a shipment from us or enter into a contract with us, we process your **identification and contact details and the data about ordered services** on the basis of our legitimate interests (without your consent) for the purpose of pursuing and protecting legal claims, our internal records, statistics and checks, for our internal administrative purposes within the cargo-partner and nippon express group, satisfaction survey aiming at the improvement of the services provided, as well as at marketing activities (information about similar goods or services as those you purchased) via e-mail, or over the phone. Our legitimate interests here are the protection of legal claims, monitoring the proper rendering of our services, direct marketing and internal administrative purposes within the group.

Processing based on compliance with legal obligations

We also have to meet certain legal obligations. If we process your personal data for this reason, we do not need to obtain your consent to such processing. On this legal basis, we process your identification and contact details and data about ordered services in order to mainly comply with the following legal regulations: Act No. 40/1964 Coll. Civil Code, Act No. 513/1991 Coll. Commercial Code, Act No. 250/2007 Coll. on consumer protection (if you order transport as a natural person), Act No. 222/2004 Coll. on value added tax, Act No. 431/2002 Coll. on accounting, Act No 395/2002 Coll. on archives and registers, IATA Rules on Air Transport, EU regulations against terroris and money laundering as amended, etc.

If you are the consignor or consignee and you ask us to have your shipment arranged by us

If you are the consignor or consignee and you ask us to have your shipment arranged by us, we process your **identification and contact details**:

For the purpose of fulfilling a shipment contract, for the purpose of arranging transport and tracking the shipment;

For the purpose of fulfilling legal obligations, in particular under Act No. 222/2004 Coll. on value added tax as amended, and Act No. 431/2002 Coll. on accounting as amended;

To protect legal claims and our internal records and for the purposes of our statistics and monitoring; our legitimate interests here are the protection of legal claims and the monitoring of the proper provision of our services.

If you communicate with us through various channels

If you communicate with us through various channels, in particular over the phone, e-mail, our website, social networks, we will process **your identification and contact details and records of the communication made** on the basis of our legitimate interests (i.e. without your consent) for the purposes of: Meeting your requirements; if you have ordered shipment with us or have entered into any other contract with us and your request relates to this contract, we may perform this processing on the basis of the performance of a contract with you;

Recording your requests so that we can check that we meet them properly and in a timely manner;

Proving that we have accepted and processed your request, e.g. when you order some goods with us this way or make a complaint;

Their analysis so as to improve the quality of our services.

If you visit our premises

If you visit our branch or its surroundings, we will process a recording from the CCTV camera system where you can be captured on the basis of our legitimate interest (i.e. without your consent) in order to protect our and your property and the life and health of persons moving in and around the branch, as well as to prove and investigate the circumstances of a potential damage.

For this purpose, we keep camera records for 30 days. If a record is used in criminal or other proceedings to prove the circumstances of a damage, crime, offence etc., we keep those for as long as necessary for the purpose given.

If you visit our warehouse premises, we will process your forename, surname and signature in the written records of warehouse entries based on our legitimate interest (i.e. without your consent) for the purpose of protecting our property and on the basis of compliance with a legal obligation (i.e. without your consent) in order to ensure the safety of and protect the lives and health of persons for the period specified by law during which we are obliged to retain such data.

If you visit an event organised by our company

If you visit an event organised by our company, we will process photos and videos on which you can be captured based on our legitimate interest (i.e. without your consent) for the purpose of promoting our company, informing about our activities, building the public, business partners' and potential employees' awareness of our activities to the extent necessary by producing such photos and videos and publishing them on various communication channels (website, social networks, Intranet, etc.) and to that connected photo and video documentation archiving. Photographs and/or videos will always be published to the extent necessary to fulfil the stated purpose and will not in any way negatively influence the privacy or dignity of the persons captured in photos and videos or otherwise violate their personality protection rights.

We process your data for the given purpose only for the period necessary to achieve the purpose of its processing, archiving included. Personal data shall be disposed (deleted) without delay after the purpose (or the legal reason) of the processing has ceased to exist, or after the expiry of the statutory period for which we are obliged to retain such data if such a legal obligation applies to us.

If you send us a notification of a suspected anti-social activity (whistle-blowing)

If you send us a notification of a suspected anti-social activity, we will process your personal data on the basis of compliance with a legal obligation (i.e. without your consent) for the purposes of:

Receiving and verifying the notification submitted through an internal notification screening system pursuant to the relevant provisions of Act No. 54/2019 on the protection of whistle-blowers as amended (hereinafter referred to as the "**Whistle-Blower Protection Act**"),

Keeping records of the data on received notifications in accordance with the Whistle-Blower Protection Act; Compliance with other obligations imposed on our company by the Whistle-Blower Protection Act or related legislation.

In connection with the registration of the data on received notifications, we are obliged to keep notifications submitted through the internal notification screening system and the documents related to the notification for the period of 3 years from the date of such notification receipt.

We process personal data to the following extent: whistle-blower's forename, surname and residence or other data from which their identity can be established if we are aware of this information. Furthermore, the identification of the person against whom the notification was made if his or her identity is known.

If you are not using our services yet

If you have not used our services yet (you do not have a shipping contract with us or have not ordered any shipment with us) and you give us your consent when providing your data we may use your **identification and contact details** for direct marketing purposes (for sending offers) by e-mail or a text message and to notify you of our offers over the phone or using other electronic means. We can also send such offers to you by mail. Your consent is voluntary and can be withdrawn at any time. To withdraw consent, please contact us as described in the "[How can individual rights be exercised?](#)" section. Withdrawal of one's consent does not affect the lawfulness of the processing until the moment of such withdrawal.

Your consent is not required for the use of your **published contact details** for the purposes of direct marketing (sending offers) by e-mail, text or multimedia messages if you are **a natural person - entrepreneur or a person authorised to act on behalf of a legal entity**. You have the right to refuse such use of contact details at any time.

How long do we process your personal data?

We process your data for a given purpose only for the period necessary to achieve the purpose of such data processing, archiving included, yet no longer than 10 years after the end of the business relationship and settlement of all related obligations arising from such a business relationship (unless the law provides for a longer period of time). The personal data used to send offers is processed for a period of 5 years from granting one's consent, unless it is processed on the basis of a business relationship (i.e. on the basis of contract performance) or after the termination of such a business relationship for the period of 10 years on the basis of our legitimate interest in the development of our business activities. Personal data is disposed (deleted) without delay after the end of the purpose (or a legal reason) of the processing or after the expiry of the statutory period during which we are authorised or obliged to process such data.

Who processes your personal data and to whom do we provide it?

All the mentioned personal data is processed by us as the controller.

We may also disclose your personal data to other entities that act as the **controller** as follows:

If you are the sender or recipient of a service ordered by us, we may provide personal data to our partners who are involved in such service performance, as described in the "[If you are the consignor or consignee and ask us to have your shipment arranged by us](#)" section, namely to the partners providing transport and delivery of parcels, e.g. to our partner abroad involved in international transport, to a courier;

As part of the fulfilment of our legal obligations towards the administrative and state authorities if we have such an obligation or if we are called upon to do so.

We also transfer personal data within the cargo-partner and nippon express group. The transfer of data within the group takes place mostly in the case of products or services the subject of which is international transport and without which it is impossible to provide a service or a product. In particular, it concerns the transfer of contact or identification details to other group companies that perform freight forwarding services for our company in the final destination, on the basis of the fulfilment of a contractual obligation or on the basis of a legitimate interest for the administrative and statistical needs of the group and, where appropriate, the provision to the controllers within the group for the purpose of shipment delivery. Furthermore, the processing based on a legitimate interest or compliance with a legal obligation aimed at ensuring security may be considered.

For the processing of personal data, we also use the services of other third parties who process personal data on our own behalf only according to our instructions and for the purposes described in the “Why we process personal data and what entitles us to do so?” section. Such **third parties** are mainly lawyers, tax advisors or auditors.

From what sources do we collect personal data?

In most cases, we process personal data that you provide to us as part of the service ordering process or when communicating with us. If you are the consignor or consignee we perform transport for we collect your data from the person/entity that has ordered the shipment.

Transferring personal data outside the EU and the EEA

As part of the provision of data to the recipients stated in the “Who processes your personal data and to whom do we provide it?”, we may also transfer your data to third countries outside the EU and the European Economic Area that do not guarantee an adequate level of personal data protection. We will only make such transfers if it is necessary for the performance of a contract between you and us as the controller, for the implementation of pre-contractual measures taken at your request as the data subject, for entering into and performing a contract entered into in your interest between us and another person/entity or if such transfer is necessary for the establishment, exercise or defence of our legal claims. In addition to these cases, we may also make such a transfer on the basis of your explicit consent after providing information about the risks associated with such transfer. In other cases of transfers of personal data outside the EU and the EEC, the conclusion of the Standard Contractual Clauses is followed.

What rights do you have when your personal data is being processed?

Right of access (Art. 15 of the GDPR) – the right to obtain confirmation of the processing or not processing of your personal data as well as for access to your personal data which we process;

Right to rectification (Art. 16 of the GDPR) – if you discover that your personal data that we process is inaccurate or incomplete, you have the right to have such data rectified or supplemented without delay;

Right to erasure or restriction of processing (Articles 17 and 18 of the GDPR) – the right to erasure or restriction of processing of your personal data if the conditions laid down by law are met;

Right to data portability (Art. 20 of the GDPR) – the right to receive from us all your personal data that you have provided to us and which we process on the basis of your consent or on the basis of the performance of a contract. We will provide you with your personal data in a structured, commonly used and machine-readable format. In order to be able to transfer data easily upon your request, it may only be data that we process in an automated manner in our electronic databases;

Right to object to processing (Art. 21 of the GDPR) – the right to object to the processing of personal data based on our legitimate interest, including objecting to processing for direct marketing purposes;

Right to lodge a complaint with a supervisory authority (Article 77 of the GDPR) – the right to lodge a complaint with the Personal Data Protection Authority of the Slovak Republic, which is located at Hraničná 12, 820 07 Bratislava. You can exercise this right in particular if you believe that we process your personal data unlawfully or in violation of the generally binding legal regulations.

How can your rights be exercised?

In all matters related to the processing of your personal data by cargo-partner SR, s.r.o., you can contact us at integrity.sk@cargo-partner.com or contact us at + 421 (0) 2 68242 300.

We will process your request without delay, yet not later than in one month. In exceptional cases, especially due to the complexity of your request, we are entitled to extend this period by extra two months. Naturally, we will inform you of such a possible extension and provide its justification.

Effective from: 27/03/2024.

16 Annex 7 – NOTIFICATION OF PERSONAL DATA SECURITY BREACH (SPECIMEN)

Personal Data Protection Authority of the Slovak Republic
Hraničná 4826/12
820 07 Bratislava

[DATE]

Re: Subject: Notification of personal data security breach

Dear Sir/Madam,

Under Article 33, par. 1 of the GDPR, *in the event of a breach of personal data protection, the controller shall, without delay and where possible not later than 72 hours after becoming aware of this fact, notify the supervisory authority of the personal data protection breach pursuant to Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.*

Controller, which is cargo-partner SR, s.r.o., registered office: Kopčianska 92, 851 01 Bratislava, Company ID: 31 358 152, entered in the Business Register maintained by the Bratislava III City Court, Part. SRO, Entry No.: 5741/B, on [DATE] at [TIME], detected a personal data breach. Within the meaning of the above-mentioned provision

of the Regulation, the Controller hereby informs the competent Personal Data Protection Authority of the following:

•Nature of the infringement

[provide the description of the nature of the personal data breach including, where possible, the categories and the approximate number of data subjects concerned and the categories and approximate number of the personal data records concerned]

•Contact point for further information

[insert the name, surname and contact details of the person from whom more information may be obtained]

•Likely consequences of the infringement

[provide the description of the likely consequences of the personal data breach]

• Measures taken

[provide the description of the measures taken or proposed by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate its potential adverse consequences]

Yours Faithfully,

cargo-partner SR, s.r.o.

[Forename, surname, position]