Pursuant to Trade Secrets Act (Official Gazette of the Republic of Slovenia, no. 44/2019) and Article 2 of the Rules of procedures regulating the work of the management board of the company Luka Koper, d.d., the company's management board adopted on 15 Oct 2019 the following

# REGULATIONS ON TRADE SECRETS PROTECTION

## SECTION 1
## GENERAL PROVISIONS

### Article 1

The present Regulations govern the area of trade secrets and the rules for their identification and protection against unlawful acquisition, use and disclosure. These Regulations also provide the common basis and a uniform system to be applied for identification, protection and access to data representing trade secrets applied in the business operations of the company Luka Koper, d.d. (hereinafter referred to as "Company").

### Article 2

The following terms, applied in these Regulations, shall have the following meaning:

1. **Trade secret** comprises the undisclosed know-how, experience and business information and shall meet the following requirements:

- is a secret in the sense that it is not known or readily accessible to a circle of persons usually dealing with this kind of information;
- has a commercial value;
- has been subject to reasonable steps, by the trade secret holder, to keep it secret.

It shall be presumed that the requirement from third indent of the previous paragraph is met if the trade secret holder has classified the information as trade secret in writing and has informed all persons who come into contact or are acquainted with it, especially the shareholders, employees, members of company bodies and other persons, about its confidentiality.

Know-how, experience and business information representing a trade secret, irrespective of the form in which they were communicated, shall be deemed to represent a commercial value for the company only as far as they represent a competitive advantage. Irrespective of the above, the competitive advantage shall not be the only method for demonstrating the commercial value.

It shall be deemed that each Company's internal information represents a trade secret since it has an impact on the market value of the company's financial instruments.

2. **Document** is each written, drawn, printed, copied, filmed, photographed, optical or any other record of content which can contain a trade secret.

3. **Media** is any means which can contain a trade secret.

4. **Identification of trade secret** is a process in which an information is classified as trade secret and is attributed a level of confidentiality and duration of confidentiality in line with these Regulations.

5. **Termination of confidentiality** of a trade secret shall mean the declassification of a confidential data into a publicly accessible data.

6. **Treatment of trade secret** shall mean the identification, labelling, accessibility, application, recording, reproduction, transmission, transfer, destruction of trade secret carriers, storage, archiving and other measures and processes which grant the security and confidentiality of trade secrets.

7. **Information Communication Technology – ICT** includes a range of computer-, IT- and communication devices (i.e. hardware), as well as applications (i.e. software), networks (i.e. Internet) and services applied for the creation, processing, transfer and storage of data.

8. **Local Area Network – LAN** is a private communication network established within a certain Company's building or area at a precise geographical location and with a uniform administration.

9. **Management board** is the Company's management body formed in line with the provisions of the applicable legislation and the Company's articles of association.

10. **Persons authorised to deal with a trade secret** shall be the members of the management board in their capacity as Company's management body, as well as the heads of organisational units (hereinafter referred to as "Heads of OU") for the field of work performed in their unit and other employees of Luka Koper, d.d. based on a written authorization of the Company's management board or Head of OU's authorization granted in line with the provisions of these Regulations.

11. **Holder of trade secret** (hereinafter referred to as "Trade secret holder") is a natural or legal person with a lawful control over the trade secret.

12. **Infringer of trade secret** (hereinafter referred to as "Infringer") is any natural or legal person who unlawfully acquires, uses or discloses a trade secret.

13. **Infringing goods** are the goods whose form, characteristics, operation, production process or marketing were seriously affected by the unlawful acquisition (misappropriation), use or disclosure of trade secret.

## Article 3

## LAWFUL ACQUISITION, USE AND DISCLOSURE OF A TRADE SECRET

(1) The acquisition of a trade secret is considered lawful when the trade secret is obtained by:
- independent discovery or creation;
- observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret;
- exercise of the right of workers or workers' representatives to information and consultation in accordance with applicable legislation, when the purpose of disclosure is to meet the above-stated purpose;
- any other practice which, under the circumstances, is in conformity with honest commercial practices, or
- exercise of the right to access public information.

(2) As lawful acquisition shall equally be considered the acquisition, use or disclosure of a trade secret whenever such acquisition, use or disclosure are permitted by the European Union or national law, or have been imposed on the party by a final and enforceable judgement, or if this be required by the investigation commission of the Parliament of the Republic of Slovenia for the purpose of enquiry carried out in line with the law regulating the parliamentary enquiry.

**Article 4**

As trade secret cannot be considered information that according to the law is public information, or information on infringement of law or infringement of honest commercial practices.

Equally, as trade secret cannot be considered any information that according to the law is designated as public.

**Article 5**

**UNLAWFUL ACQUISITION, USE AND DISCLOSURE OF TRADE SECRETS**

The acquisition of a trade secret is unlawful if:

- carried out by unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files containing the trade secret or from which the trade secret can be deducted, or by any other conduct which is considered contrary to honest commercial practices.

- acquired by a person who used or disclosed the trade secret unlawfully, whenever a person, at the time of the acquisition, knew or ought, under the circumstances, to have known that the trade secret had been obtained from another person who was using or disclosing the trade secret unlawfully.

The use or disclosure of a trade secret shall be considered unlawful if applied or disclosed by a person who meets any of the following conditions:
- having acquired the trade secret unlawfully;
- being in breach of a confidentiality agreement or any other duty not to disclose the trade secret;
- whenever a person, at the time of use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained from another person who was using or disclosing the trade secret unlawfully.

The production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods for those purposes, shall also be considered as unlawful use of a trade secret where the person carrying out such activities knew, or ought, under the circumstances, to have known that the trade secret was used unlawfully.

**Article 6**

Pursuant to applicable law and Company's by-laws, those obliged to protect the Company's trade secret shall be:
- all Company's employees;
- all Company's bodies (supervisory board, management board, workers' council);
- all legal and natural persons that due to the nature of their work and based on their business cooperation with the Company receive the data classified as trade secret.

Each person that has been entrusted an information classified as trade secret or has been acquainted with the content of such information, shall be responsible for its protection and maintaining of its confidentiality.

**Article 7**

Pursuant to the provisions of these Rules, a determined level of trade secret confidentiality can be attributed to an information (hereinafter referred to as "confidential information") whose content is so important that its disclosure to an unauthorized person would cause or might cause clear adverse consequences to the Company, to its economic interests and competitive advantages.

**Article 8**

Persons who fill a determined position or are employed within the Company, as well as legal and natural persons outside the Company shall be obliged to protect the trade secret, irrespective of how they were acquainted with it.

The obligation of professional secrecy shall not cease even when the person who fills a determined position or is employed within the Company ceases to perform this position. The person shall be obliged to protect the trade secret until it is declared non-confidential, or is disclosed by the Company's authorized person or ceases to be confidential in a legal manner, independently from the Company.

The obligation of professional secrecy of legal and natural persons outside the Company who were transmitted the trade secret by the Company, shall not cease with the termination of the legal transaction or finalisation of legal transaction for which the trade secret was communicated to them. On the contrary, the obligation of professional secrecy shall terminate only when declassified as confidential by the Company, or when disclosed by authorized person in the Company, or when the trade secret ceases to be confidential in a legal manner independently from the Company, or when the period of legal transaction in which the information was classified as trade secret, expires.

All employees shall be obliged to estimate the level of sensitivity of information within the framework of their tasks and competences, and they shall propose to authorized persons to classify determined information as confidential, if in their opinion this is considered necessary.

**SECTION II**
**IDENTIFICATION OF TRADE SECRET**

**Article 9**

The level of confidentiality of a trade secret shall be determined by the authorized person based on the conditions and in the manner defined herein.

**Article 10**

The authorized person shall determine the level of confidentiality of a trade secret on its occurrence or at the beginning of implementation of a task resulting in confidential data.

When determining the confidentiality level of a trade secret, the authorized person must assess the possible adverse consequences for the Company in case the information is disclosed to an unauthorized person. Based on this assessment, the information classified as trade secret shall be attributed the level

of confidentiality and the conditions for confidentiality expiration, and the trade secret shall be properly labelled, as provided for in these Regulations.

The assessment based on which a confidentiality level is attributed to a trade secret shall be made in writing.

Whenever the elaboration of assessment prior to the implementation of urgent tasks makes it difficult or impossible to implement the above-stated urgent tasks, the authorized person can attribute the confidentiality level to an information orally, and shall label the document appropriately. The written assessment shall be provided as soon as possible, but not later than three days.

**Article 11**

The authorized person shall identify as confidential also the data resulting from merging or linking of data which originally were not confidential but once merged or linked represent a data or a document which needs to be protected due to reasons stated herein.

When confidential data is contained only in a minor part of a document or in an individual document, this has to be excluded from the rest and treated as required by the attributed level of confidentiality. If exclusion is not possible, the level of confidentiality shall apply to the entire document.

**Article 12**

By considering the adverse effects that disclosure of confidential data to unauthorized persons might cause to the Company, the trade secrets from the Article 5 above shall be attributed one of the following confidentiality levels:

**1. SECRET** – shall be attributed to a trade secret which disclosure to unauthorized persons can cause serious damage to the security or commercial interests of the Company, or can cause **a very significant** damage to the Company, a loss of its competitive advantage or can harm its reputation;

**2. CONFIDENTIAL** – shall be attributed to a trade secret which disclosure to unauthorized persons can cause damage to the security or commercial interests of the Company, or can cause **a significant** damage to the Company, a loss of its competitive advantage or can harm its reputation;

**3. INTERNAL** – shall be attributed to a trade secret which disclosure to unauthorized person can cause damage to the operation or implementation of tasks of the Company or part of the Company, or can cause the Company or its single organisational unit a loss, a loss of its competitive advantage or can harm its reputation.

For attributing confidentiality levels to Company's trade secrets only the levels stated above shall be applied.

**Article 13**

When attributing the confidentiality level, the authorized person shall define the lowest level which still guarantees the data security that is required for the protection of Company’s interests and its security.

The document which is formed of data already classified as confidential shall be attributed at least the same level of confidentiality and duration of confidentiality as applies to the data with the highest level and duration of confidentiality contained in the same document.

**Article 14**

The level of confidentiality can only be modified by the authorized person who determined the level of confidentiality.

The grounds for changing the confidentiality level must be given in writing. The authorized person shall modify the confidentiality level of the data as soon as the conditions for attributing individual confidentiality levels stated herein are changed. The information concerning the changed confidentiality level shall be circulated to all persons who received or have access to confidential data.

**Article 15**

Each confidential data and each document containing confidential data shall be labelled with the confidentiality level and organisational unit details, if this is not apparent, and it shall state the names of the persons who received the document labelled as confidential.

The designations stated above shall be applied in a manner that is appropriate for the type of media and its characteristics.

An information or document shall be treated as confidential also if labelled only as **TRADE SECRET**.

**Article 16**

The confidentiality of data shall cease:

- on the date stated in the document, if stated;
- on the occurrence of a law or legal provision adopted by a state body stating that the information is to be disclosed to the public;
- on revocation of confidentiality by the Company's competent body.

When the termination of confidentiality cannot be defined as stated in the paragraph above because of the nature or content of the data, the confidentiality shall cease on the expiration of the time limit stated in the regulation applying to archival documents and archives in general.
The data representing a trade secret and labelled with **»TRADE SECRET – CONFIDENTIAL«** confidentiality level shall be examined by the authorized person once a year, whereas other data with other confidentiality levels shall be examined every three years in order to assess whether the reasons for treating these data as confidential still exist.

The authorized person can change the conditions set for the termination of the trade secret providing that there are reasonable grounds for termination of confidentiality. In such a case, the authorized person shall immediately notify all persons who received the trade secret or have access to it.

**Article 17**

The eligible user of confidential data who received the data in legitimate manner may propose to the authorized person the revocation or declassification of confidentiality level if in his/her opinion the confidentiality of data is not justified or appropriately attributed.

The authorized person is obliged to consider the proposal from the previous paragraph and inform the submitting party about his/her decision.

## SECTION III
## ACCESS TO TRADE SECRETS AND THEIR PROTECTION

### Article 18

The right to access trade secrets is only held by individuals who must be acquainted with them due to the filling of their position, or because of their implementation of tasks or due to their business cooperation with the Company.

### Article 19

While taking over their position or prior to the beginning of their business cooperation with the Company, the individuals from the previous Article shall sign a statement in which they confirm their acquaintance with these Regulations and other provisions regulating the protection of Company's trade secrets emerging during their filling of position or cooperation with the Company, and they shall declare their commitment to treat these data in line with these provisions.

### Article 20

A person who during the implementation of his/her work becomes acquainted with the data designated as trade secrets is not allowed to use these data for any other purpose other than for the implementation of his/her working duties or filling of position.

### Article 21

The authorised person from the organisational unit shall provide for an accurate record and control over all confidential data distributed outside the organisational unit. From the record shall emerge when and to whom were the confidential data transmitted. The record can be kept either in electronic form or in paper.

### Article 22

Based on these Regulations and rules adopted on their basis, each organisational unit shall establish a system of procedures and measures for ensuring the protection of trade secrets in line with the corresponding trade secret confidentiality level which prevents their disclosure to unauthorized persons.

The procedures and measures from the paragraph above shall include:

- the general safety measures,
- the protection of business premises,
- the protection of documents and media containing confidential data,
- the protection of communications transmitting confidential data,
- the manner of attributing confidentiality levels,
- the protection of equipment used to process the trade secrets,
- the manner of informing the users with the measures and procedures for the protection of trade secrets,
- the control and record of accessing trade secrets,
- the control and record of transmitting and distributing trade secrets.

The authorized person shall be obliged to provide that personnel involved in the processing and protecting confidential data take part at trainings organised once every two years.

**Article 23**

On the level of the organisational unit, the data representing a trade secret shall be kept in such a way as to allow access only to authorized personnel and to those who need them for the implementation of their duties.

Data representing a trade secret can be sent outside the premises exclusively based on prescribed security measures and procedures which must guarantee that these data are accepted by authorized person or individuals who are entitled to deal with them.
Any transmission or forwarding by organisational units of confidential data via unprotected information-communication tools is forbidden.

**Article 24**

**Workers' representatives shall also be entitled to access the data classified as trade secrets while exercising the workers' rights in line with the applicable legislation, providing that these data are required to implement the purpose stated above.**

**Article 25**
**COMPETENCES AND RESPONSIBILITIES**

Those responsible for a direct implementation of proceedings and measures related to the protection of business secrets shall be:
- the Company's management board that shall provide the conditions for the implementation of these Regulations and rules,
- other Company's bodies,

- Heads of organisational units of Luka Koper d.d. that are responsible for:
  1. adequate treatment of data classified as trade secrets;
  2. attribution of confidentiality levels;
  3. establishing and keeping a record of documents representing trade secrets and access to them;
  4. issuing of authorizations in case of substitution of Head of OU or issuing of authorizations for determined operations stated herein, required to protect the trade secret;
  5. protection and storage of data classified as trade secret;
  6. training and education of employees concerning trade secret protection;
  7. control over the treatment of trade secrets;
  8. providing information and taking of measures in case of loss or disclosure of business secrets;

- Authorised persons (Security and Safety, and IT) that are responsible for:
  1. control and reporting to the Company's management board on deficiencies, by proposing solutions for efficient implementation of these Regulations and instructions.
  2. elaboration of a 'Plan for protection of trade secret', to be approved by the management board. The Plan for protection shall be attributed the level BUSINESS SECRET – CONFIDENTIAL.
  3. implementation of measures in cases where there is a suspicion of business secret being disclosed to unauthorized persons.

**Article 26**

Each employee of Luka Koper d.d. who discovers that confidential data were lost or disclosed to unauthorized persons shall immediately notify the head of the organisational unit in which he/she is employed.

Persons who perform determined functions in the Company (i.e. in the Company's bodies or are representatives of organisational units) or persons doing business with the Company who discover that confidential data were lost or disclosed to unauthorized person shall immediately notify the employee from Luka Koper d.d. with whom they do business or the head of organisational unit in charge of security (i.e. Port Security).

The head of organisational unit or the person performing a function in a Company's body in which a disclosure of confidential data took place shall cooperate with authorized persons from Luka Koper d.d. who are in charge of Security & Safety and IT, and they shall immediately take all further measures necessary to investigate the circumstances in which confidential data were lost or disclosed to an unauthorised person, in order to prevent adverse consequences and further loss or unauthorized disclosure of confidential data.

**SECTION IV**
**CONTROL**

**Article 27**

The persons in charge of exerting internal control over the implementation of these Regulations and rules adopted on their basis shall be:

- the authorized persons from organisational units, and
- the authorised persons (responsible for Safety & Security, and responsible for IT) on the level of Luka Koper d.d.

**SECTION V**
**VIOLATION OF PROVISIONS OF THESE REGULATIONS**

**Article 28**

Any violation of the provisions of these Regulations and any violation of the rules adopted on their basis shall represent a breach of national legislation as well as infringement of labour law and employment contract.

A person who violates the legal provisions stated above shall be liable to disciplinary action, payment of compensation and shall be held criminally responsible.

**APPLICATION OF LEGAL REMEDIES**

**Article 29**

(1) In the proceedings related to trade secret infringement, the legal provisions regulating the civil procedure shall be applied, unless otherwise provide by law.

(2) In the proceedings for granting interim relief, the legal provisions regulating the enforcement and security shall be applied, unless otherwise provided with the Trade Secret Act.

**TRANSITIONAL AND FINAL PROVISIONS**
**Article 30**

The management board shall adopt a special written instruction setting out precisely:

- the ways and the forms applied for labelling data and documents containing trade secrets with confidentiality level,
- the procedures and the measures for dealing with confidential data,
- the way of keeping a record of documents classified as trade secrets with a determined confidentiality level, and access to them,
- the way and the operational content of internal control over the implementation of these Regulations and rules adopted on their basis.

**Article 31**

**The measures for physical and technical protection and the measures for the treatment of trade secrets shall be implemented within six (6) months as of the date of approval of the Plan for trade secrets protection.**

These Regulations shall become effective on 15 Oct 2019 and shall remain in force until revocation.

On the day of adoption of these Regulations, the Rules on business secret adopted on 1 January 2014 shall expire.

| President of the Management Board: | Member of the Management Board: | Member of the Management Board: | Member of the Management Board – Workers' Director: |
|---|---|---|---|
| Dimitrij Zadel | Metod Podkrižnik | Irma Gubanec | Vojko Rotar |