Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR), the Personal Data Protection Act data are issued by the director of the company LSC TEH celostne rešitve d.o.o., Kranjska cesta 4, 4240 Radovljica (below: LSC TEH d.o.o.)

Rules of the personal data protection

I. GENERAL PROVISIONS

Article 1

These rules determine the technical and organizational procedures and measures for the protection of personal data in the company LSC TEH d.o.o. in order to prevent illegal, unauthorized access, processing, use or transmission of personal data, accidental or unauthorized destruction, alteration or deficiency. The measures shall be reviewed and supplemented where necessary.

Employees and external collaborators who process and use personal data in their work must be familiar with:

- EU General Data Protection Regulation (GDPR),

- the Personal Data Protection Act, together with sectoral legislation governing an individual area of their work,

- NA 101 Information security policies,

- and the content of these rules.

Article 2

Terms used in this policy have the following meanings:

· GDPR - General Data Protection Regulation (Regulation (EU) 2016/679)

· ZVOP-1 - Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 86/04 and 113/05);

· Personal data - is any data relating to an individual, regardless of the form in which it is expressed;

· Individual - is an identifiable or identifiable natural person to whom personal data relates; a natural person is identifiable if he or she can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. High cost or time consuming;

· Personal data set - is any structured set of data containing at least one personal data that is accessible on the basis of criteria that allow the use or aggregation of data, regardless of whether the set is centralized, decentralized or dispersed on a functional or geographical basis ; structured data set is a set of data organized in such a way as to determine or enable the identifiability of an individual;

· Processing of personal data - means any action or series of actions carried out in relation to personal data which are automatically processed or which are part of a personal data file or intended for inclusion in a personal data file, in particular collection, acquisition, entry , editing, storing, adapting or modifying, retrieving, viewing, using,

disclosing, transmitting, communicating, disseminating or otherwise making available, classifying or linking, blocking, anonymising, deleting or destroying; processing can be manual or automated (means of processing);

· Consent of the data subject - means any voluntary, explicit, informed and unambiguous statement of the will of the data subject by which he or she expresses consent to the processing of personal data concerning him or her by a statement or clear affirmative action. ;

· Personal data controller - is a natural or legal person or other person in the public or private sector who alone or together with others determines the purposes and means of personal data processing or a person determined by law who also determines the purposes and means of processing;

Processor of personal data - a legal or natural person or other person of the public or private sector who processes personal data on behalf of the controller of personal data;

· User of personal data - is a natural or legal person or other person of the public or private sector to whom personal data is provided or disclosed;

· Sensitive personal data - are data on racial, ethnic or ethnic origin, political, religious, philosophical beliefs, health status, sexual life, entry or deletion in or from criminal or misdemeanor records, and biometric characteristics;

· Data carrier - are all types of means on which data are recorded or recorded (documents, acts, materials, files, computer equipment including magnetic, optical or other computer media, photocopies, sound and image material, microfilms, data transmission devices , etc.);

Article 3

Description of personal data files managed by LSC TEH d.o.o. is kept in the catalog of personal data files (description of personal data files), which is kept in accordance with the provisions of Article 26 of ZVOP-1. The catalog of personal data files is updated every time the type of personal data in an individual database changes.

Employees who process personal data must be acquainted with the catalog of personal data files, and in accordance with Article 30 of ZVOP-1, access to the catalog of personal data files must also be provided to individuals to whom personal data relate upon request.

The Director is obligated to keep an up-to-date list from which it is clear for each personal data file which person is responsible for each personal data file and which persons may process personal data relating to each personal data file due to the nature of their work. The following data shall be entered in the list: the name of the personal data file, the personal name and job title of the person responsible for the personal data file and the personal name and job title of persons who may process personal data relating to the personal data file.

II. LEGAL PROCESSING

Article 4

Personal data are processed only if required by law or if the personal consent of the individual is given for the processing of certain personal data. The personal data processed must be accurate and up-to-date.

III. PROTECTION OF PREMISES, COMPUTER EQUIPMENT, PROTECTION OF SYSTEM AND APPLICATION SOFTWARE COMPUTER EQUIPMENT AND DATA PROCESSED WITH COMPUTER EQUIPMENT

Article 5

Protection of premises and computer equipment or all organizational and physical and / or technical measures are implemented in accordance with the Information Security Policy (ISO 27001).

IV. SERVICES PROVIDED BY EXTERNAL LEGAL OR NATURAL PERSONS

Article 6

A written contract provided for in Article 28 of the General Data Protection Regulation shall be concluded with any external legal or natural person who performs individual tasks related to the collection, processing, storage or transmission of personal data (processor). Such a contract must also prescribe the conditions and measures to ensure the protection of personal data and their protection. Prior to concluding a contract with the processor, the responsible person (usually the head of the department) is obligated to obtain information from the processor, which enables verification of whether the processor meets the requirements of legislation in the field of personal data protection; this also includes the disclosure of all subcontracted processors, including their titles and locations.

The mere possibility of access to data, even at the express request of the company (e.g. as part of a service intervention on hardware, etc.), is considered contractual processing within the meaning of paragraph 1 of this article.

Processors may provide personal data processing services only within the scope of the Client's authorization and may not process or otherwise use the data for any other purpose to which they are bound by the contract.

Authorized legal or natural person who for LSC TEH d.o.o. performs the agreed services outside the controller's premises, must have at least the same strict method of personal data protection as provided for in these regulations and the Information Protection Policy (ISO 27001).

In addition to other requirements, the company must guarantee in contracts with processors the right to carry out a review or audit in the field of personal data protection at least once a year with the contracted processor. An inspection or audit must be carried out whenever there is any suspicion or indication that the processor is in breach of contract or that it does not ensure a sufficient level of protection of personal data. The audit is carried out at the expense of the company, and the processor may not charge the company for the possible engagement of its people and / or subcontracted processors.

V. RECEIPT AND TRANSMISSION OF PERSONAL DATA

Article 7

The employee in charge of receiving and recording mail must deliver the postal item with personal data directly to the individual or to the service to which the item is addressed.

The employee in charge of receiving and recording mail opens and inspects all postal items and items that otherwise arrive at LSC TEH d.o.o. they are brought by customers or couriers, except for the consignments referred to in the third and fourth paragraphs of this Article.

The employee in charge of receiving and recording mail shall not open those items which are addressed to another body or organization and which are delivered by mistake and items which are marked as personal data or for which the indications on the envelope indicate that they relate to competition or call.

The worker in charge of receiving and recording mail may not open consignments addressed to the worker stating on the envelope that they are to be served in person on the addressee, and consignments which first state the personal name of the worker without indicating his official position and only then the address LSC TEH d.o.o.

Article 8

Personal data and sensitive personal data may be transferred by information, telecommunication and other means only when carrying out procedures and measures that prevent unauthorized persons from misappropriating or destroying data and unjustifiably disclosing their content (appropriate cryptographic methods and password protection).

Sensitive personal data shall be sent in physical form to the addressees in sealed envelopes against signature in the delivery book or by delivery note. The envelope in which personal data are transmitted must be made in such a way that the envelope does not allow the contents of the envelope to be visible under normal light or when the envelopes are illuminated with normal light. The envelope must also ensure that the opening of the envelope and acquaintance with its contents cannot be carried out without a visible trace of the opening of the envelope.

Article 9

The processing of sensitive personal data must be specially marked and secured in accordance with the Information Security Policy (ISO 27001).

The data referred to in the preceding paragraph may be transmitted over telecommunication networks only if they are specially protected by cryptographic methods and in such a way as to ensure the illegibility of the data during their transmission.

Article 10

Personal data are provided only to those users who prove themselves with an appropriate legal basis or with a written request or consent of the data subject.

For each transfer of personal data, the beneficiary must submit a written application, which must clearly state the provision of the law authorizing the user to obtain personal data, or the application must be accompanied by a written request or consent of the data subject.

Each transfer of personal data is recorded in the records of transfers, from which it must be evident which personal data were transferred, to whom, when and on what basis (Article 22 of ZVOP-1).

VI. DELETE DATA

Article 11

Personal data are stored only for as long as necessary to achieve the purpose, after fulfilling the purpose of processing personal data are deleted, destroyed, blocked or anonymized, if not defined by the law governing archives as archives or if the law for individual does not specify the type of personal data otherwise.

The deadlines for deleting personal data from the database can be seen in the document Catalog of personal data files (seventh indent in Table 2. Data on the personal data file - Retention period).

Article 12

To delete data from computer media, such a method of deletion is used that it is impossible to restore all or part of the deleted data.

Data on traditional media (documents, files, etc.) are destroyed in a way that makes it impossible to read all or part of the destroyed data. Auxiliary material is destroyed in the same way (e.g. inspection certificates, inspection orders, etc.).

When transferring personal data carriers to the place of destruction, it is necessary to provide adequate security during the transfer.

The transfer of data carriers to the place of destruction and the destruction of personal data carriers shall be supervised by the director or a person authorized by him in writing, who shall also draw up an appropriate report on the destruction.

VII. ACTION ON SUSPECT OF UNAUTHORIZED ACCESS

Article 13

Employees are obliged to immediately notify an authorized person or supervisor of activities related to the discovery or unauthorized destruction of confidential information, malicious or unauthorized use, misappropriation, alteration or damage, and they themselves try to prevent such activity.

In the event of a personal data breach, the controller shall notify the competent supervisory authority without undue delay, and preferably no later than 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to jeopardize the rights and freedoms of individuals. Where no notification is given to the supervisory authority within 72 hours, it shall be accompanied by an indication of the reasons for the delay.

VIII. RESPONSIBILITY FOR IMPLEMENTING SECURITY MEASURES AND PROCEDURES

Article 14

The director of the company is responsible for supervising the implementation of procedures and measures for the protection of personal data, who may authorize other persons who are not employees of the company for individual tasks.

The supervision referred to in paragraph 1 of this Article shall also include procedures for regular testing, evaluation and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing. All employees and other persons in the company are obliged to participate in this.

Article 15

Everyone who processes personal data is obliged to carry out the prescribed procedures and measures for data protection and to protect data of which he or she was aware or was acquainted with them in the performance of his or her work. The obligation of data protection does not end with the termination of the employment relationship.

Before starting work at the workplace where personal data are processed, the employee must sign a special statement committing him to the protection of personal data. The statement may also be part of the employment contract.

It must be evident from the signed statement that the signatory is acquainted with the provisions of these rules and the provisions of the GDPR and the applicable personal data protection law, and the statement must also include instructions on the consequences of the breach.

Article 16

Employees are disciplinary liable for violating the provisions of the previous article, while others are subject to contractual obligations.

IX. FINAL PROVISIONS

Article 17

This policy is valid and applicable from 1.2.2022 onwards.

Article 18

These rules are located in the company's document system, and all employees can also see them at the company's management.