On the basis of 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, hereinafter referred to as GDPR), and the Personal Data Protection Act, the Director of LSC GROUP celostne rešitve d.o.o., Kranjska cesta 4, 4240 Radovljica (hereinafter referred to as LSC GROUP d.o.o.) issues the following

# Personal Data Protection Policy

## I. GENERAL PROVISIONS

### 1. article

This Policy establishes the technical and organisational procedures and measures for the protection of personal data in LSC GROUP d.o.o. in order to prevent unlawful and unauthorised access, processing, use or disclosure of personal data, accidental or intentional unauthorised destruction of data, alteration or loss. The measures shall be reviewed and updated whenever necessary.

Employees and external collaborators who process and use personal data in the course of their work shall be made aware of:
- The EU General Data Protection Regulation (GDPR),
- the Personal Data Protection Act, together with the sector-specific legislation governing their particular area of work,
- NA 101 of the Information Security Policy,
- and the contents of this policy.

### 2. article

As used in these Regulations, the following terms shall have the following meanings:

- **GDPR** - General Data Protection Regulation (Regulation (EU) 2016/679)
- **ZVOP-2 -** Personal Data Protection Act (Official Journal of the Republic of Slovenia, No. 163/22);
- **Personal data** - is any data relating to an individual, regardless of the form in which it is expressed;
- **Individual** - means an identified or identifiable natural person to whom personal data relate; 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, where the means of identification are not costly or time-consuming;
- **A personal data set** - is any structured set of data containing at least one personal data which is accessible on the basis of criteria that allow the data to be used or aggregated, whether the set is centralised, decentralised or dispersed on a functional or geographical basis; a structured set of data is a set of data that is organised in such a way as to identify or make identifiable an individual;
- **Processing of personal data** - means any operation or set of operations which is performed upon personal data which are subject to automated processing or which, when manually processed, form part of, or are intended to form part of, a personal data file, in particular collection, retrieval, recording, adaptation, storage, alteration, retrieval, consultation, use, disclosure by transmission, communication, dissemination or otherwise making available, classification or association, blocking, anonymisation, erasure or destruction; the processing may be manual or automated (means of processing);
- **Data subject consent -** means any voluntary, explicit, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies his or her agreement to the processing of personal data concerning him or her;

- **Data controller** - means the natural or legal person or other person in the public or private sector who, alone or jointly with others, determines the purposes and means of the processing of personal data, or the person designated by law who also determines the purposes and means of the processing;
- **Personal data processor** - a legal or natural person or other public or private sector entity that processes personal data on behalf of the personal data controller;
- **User of personal data** - means a natural or legal person or other person in the public or private sector to whom personal data are provided or disclosed;
- **Sensitive personal data** - means data concerning racial, ethnic or national origin, political opinions, religious or philosophical beliefs, health, sex life, entry in or removal from a criminal record or criminal record, and biometric characteristics;
- **Data medium** - means any type of medium on which data are recorded or reproduced (documents, deeds, papers, files, computer equipment including magnetic, optical or other computer media, photocopies, audio and visual material, microfilms, data transmission devices, etc.);

**3. article**

The description of the personal data collections of which LSC GROUP d.o.o. is the controller is kept in the catalogue of personal data collections (description of personal data collections), which is kept in accordance with the provisions of Article 30 of GDPR. The catalogue of personal data collections is updated whenever there is a change in the type of personal data in each collection.

Employees processing personal data must be familiar with the catalogue of personal data files and access to the catalogue of personal data files must also be made available to data subjects on request.

The Director is obliged to keep an up-to-date list clearly indicating, for each personal data collection, which person is responsible for each personal data collection and which persons may, by the nature of their work, process personal data relating to each personal data collection. The following information shall be entered in the list: the name of the personal data collection, the personal name and function of the person responsible for the personal data collection and the personal name and function of the persons who, by the nature of their work, may process personal data relating to the personal data collection.

## II. LAWFUL DATA PROCESSING

**4. article**

Personal data will only be processed if required to do so by law or if the processing of certain personal data is subject to the individual's personal consent. The personal data processed must be accurate and up-to-date.

## III. SECURITY OF PREMISES, COMPUTER EQUIPMENT, SYSTEM AND APPLICATION SOFTWARE COMPUTER EQUIPMENT AND DATA PROCESSED BY COMPUTER EQUIPMENT

**5. article**

The security of premises and computer equipment, or all organisational, physical and/or technical measures, shall be implemented in accordance with the **Information Security Policies (ISO 27001).**

## IV. SERVICES PROVIDED BY EXTERNAL LEGAL OR NATURAL PERSONS

**6. article**

A written contract, as provided for in Article 28 of the General Data Protection Regulation, shall be concluded with any external legal or natural person who carries out specific tasks relating to the collection, processing, storage or transfer of personal data (processor). Such a contract must also necessarily lay down the conditions and measures to ensure the protection of personal data and the safeguarding of personal data. Before concluding a contract with a processor, the responsible person (usually the head of the department) is obliged to obtain from the processor information enabling verification of the processor's compliance with the requirements of the data protection legislation; this includes disclosure of all sub-processors, including their names and headquarters.

The mere possibility of accessing data, even at the express request of the company (e.g. in the context of a service operation on hardware, etc.), shall be considered as contractual processing within the meaning of paragraph 1 of this Article.

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

An authorised legal or natural person providing agreed services for LSC GROUP d.o.o. outside the Controller's premises must have at least the same level of protection of personal data as provided for in this Policy and the **Information Security Policies (ISO 27001).**

In addition to other requirements, the Company must secure in its contracts with processors the right to have a personal data protection review or audit carried out at least once a year by the contracted processor. A review or audit must be carried out whenever there is any suspicion or indication that the processor is in breach of the contract or is not providing an adequate level of protection of personal data. The audit shall be carried out at the Company's expense and the Processor may not charge the Company for any involvement of its own people and/or sub-processors.

## V. RECEIPT AND DISCLOSURE OF PERSONAL DATA

**7. article**

The employee responsible for receiving and registering mail must hand over the postal item containing personal data directly to the individual or to the service to which it is addressed.

The employee in charge of receiving and registering mail shall open and inspect all postal items and items arriving at LSC GROUP d.o.o. by other means brought by customers or couriers, except for the items referred to in the third and fourth paragraphs of this Article.

The employee responsible for receiving and registering mail shall not open mail addressed to another authority or organisation and delivered in error, or mail marked as personal data or which, from the markings on the envelope, appears to relate to a competition or call for tenders.

The employee responsible for receiving and registering the mail may not open items addressed to an employee whose envelope indicates that they are to be delivered personally to the addressee, or items which first state the employee's personal name without indicating his/her official position and then state the address of LSC GROUP d.o.o.

**8. article**

Personal data and sensitive personal data may be transmitted by information, telecommunications and other means only if procedures and measures are in place to prevent unauthorised persons from accessing or

destroying the data and from gaining unauthorised access to its contents (appropriate cryptographic methods and password protection).

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

**8. article**

The processing of sensitive personal data must be specifically marked and protected in accordance with the **Information Security Policies (ISO 27001).**

The data referred to in the preceding paragraph may be transmitted over telecommunications networks only if they are specifically secured by cryptographic methods and in such a way as to ensure that the data are not readable during transmission.

**9. article**

Personal data shall only be disclosed to those users who provide the relevant legal basis or the written request or consent of the data subject.

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

Any disclosure of personal data shall be recorded in a record of disclosures, which must show which personal data have been disclosed, to whom, when and on what basis (Article 41 ZVOP-2).

## VI. ERASURE OF DATA

**10. article**

Personal data shall be stored only for as long as is necessary to achieve the purpose; after the purpose of the processing has been fulfilled, personal data shall be erased, destroyed, blocked or anonymised, unless they are classified as archival material under the law governing archival material or unless the law provides otherwise for specific types of personal data.

The time limits for the deletion of personal data from the database are set out in the Catalogue of personal data collections (seventh indent in Table 2.)

**11. article**

The method of erasure used to delete data from computer media shall be such that it is impossible to restore all or part of the deleted data.

Data on traditional media (documents, files, etc.) shall be destroyed in such a way that all or part of the destroyed data cannot be read. Ancillary material (e.g. certificates of inspection, inspection orders, etc.) shall be destroyed in the same way.

When personal data media are transferred to the destruction site, appropriate security shall be ensured at the time of transfer.

The transfer of data media to the destruction site and the destruction of personal data media shall be supervised by the Director or a person authorised in writing by the Director, who shall also draw up an appropriate record of the destruction.

## VII. ACTION TO BE TAKEN IN THE EVENT OF SUSPECTED UNAUTHORISED ACCESS

**12. article**

Employees shall immediately report any activity involving the discovery or unauthorised destruction of confidential information, malicious or unauthorised use, misuse, alteration or damage to an authorised person or to a supervisor and shall attempt to prevent such activity themselves.

In the event of a personal data breach, the controller shall notify the competent supervisory authority without undue delay and preferably not later than 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to jeopardise the rights and freedoms of individuals. Where notification to the supervisory authority is not given within 72 hours, it shall be accompanied by a statement of the reasons for the delay.

## VIII. RESPONSIBILITY FOR THE IMPLEMENTATION OF SECURITY MEASURES AND PROCEDURES

**14. article**

The Director of the Company is responsible for supervising the implementation of the procedures and measures for the protection of personal data and may delegate specific tasks to other persons not employed by the Company.

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

**15. article**

Anyone processing personal data is obliged to implement the procedures and measures prescribed for data protection and to safeguard the data of which he or she has knowledge or becomes aware in the course of his or her work. The obligation to protect data shall not cease upon termination of the employment relationship.

Before taking up a post in which personal data are processed, the employee shall sign a specific declaration binding him or her to the protection of personal data. The declaration may also form part of the employment contract.

The signed declaration must indicate that the signatory is aware of the provisions of this Regulation and of the provisions of the GDPR and of any applicable law on the protection of personal data, and must contain a statement of the consequences of any breach.

**16. article**

Staff members shall be liable to disciplinary action for breach of the provisions of the preceding Article, and others shall be liable on the basis of their contractual obligations.

## IX. FINAL PROVISIONS

**17. article**

These Rules shall be valid and applicable from 20.3.2024.

**18. article**

This policy is located in the company's document system and is also available for inspection by the company's management for all employees.