SAMPLE POLICY PROTECTING PERSONAL DATA

The Sample Rulebook contains an example of how to draft the Rulebook on Personal Data Protection in accordance with ZVOP-2 and the General Data Protection Regulation (GDPR).

The sample is only a suggestion, on the basis of which you can create your own Rules according to your needs. In a similar way, as follows from the sample, you formulate provisions on the way to protect personal data, in accordance with your organizational and technical procedures and data security measures.

When preparing the samples, a wide range of possibilities are taken into account, but due to the specific organizational technical and functioning of legal entities, the rules must be adjusted, according to your premises, software, possible cooperation with third parties, etc.

On the basis of _____ (e.g. company statute, decision of the head of the authority, etc.) and 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 in the processing of personal data and on the free flow of such data and on repealing Directive 95/46/EC (General Data Protection Regulation) and the provisions of the Act on the Protection of Personal Data (Official Gazette of the Republic of Slovenia, No. 163/22, hereinafter: ZVOP-2) issued by _____ (name of legal entity)

THE RULE
on securing personal data

I. GENERAL PROVISIONS

1 . Article

These regulations define the technical and organizational procedures and measures for securing LEXEU's personal data with the aim of preventing illegal and unauthorized access, processing, use or transmission of personal data, accidental or intentional unauthorized destruction of data, its alteration or loss. The measures are reviewed and supplemented when necessary.

Employees and external collaborators who process and use personal data in their work must be familiar with the General Data Protection Regulation, the Personal Data Protection Act, the regional legislation governing the individual area of their work and the content of this policy.

Article 2

The terms used in these regulations have the meaning defined by the regulations defined in Article 1, and in particular:

1. Confidential information according to this policy is information that constitutes a business secret and personal information.

2. Personal data means any information relating to an individual (hereinafter: the individual to whom the personal data relates);

3. An identifiable individual is one who can be identified directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier, or by reference to one or more factors that characterize the physical, physiological, genetic , mental, economic, cultural or social identity of that individual.

4. Controller means a natural or legal person who, alone or together with others, determines the purposes and means of processing; where the purposes and means are determined by Union law or Member State law, the controller or the specific criteria for its appointment may be determined by Union law or Member State law.

5. Collection means any structured set of personal data that is accessible according to specific criteria, and the set may be centralized, decentralized or dispersed on a functional or geographical basis.

6. Processing means any action or set of actions that interferes with personal data.

7. User means a natural or legal person, public authority, agency or other body to whom personal data has been disclosed, regardless of whether it is a third party or not. However, public authorities that may receive personal data in the context of an individual inquiry in accordance with Union law or the law of a Member State are not considered users; the processing of this data by these public authorities takes place in accordance with the applicable rules on the protection of personal data, depending on the purpose of the processing.

8. A contractual processor is a natural or legal person who processes personal data on behalf of and on behalf of the personal data manager in the field of personal data processing.

9. A contractual sub-processor is a legal or natural person to whom the contractual processor, with the consent of the controller, entrusts certain entrusted tasks.

10. Disclosure of personal information is the transmission or disclosure of personal information.

11. The data carrier is equipment through which personal data collections can be accessed, all types of means on which data is recorded or recorded (documents, materials, files, computer equipment including magnetic, optical or other computer media, photocopies, audio and visual material, microfilms, data transfer devices, etc.).

12. A third country is a country that is from Africa.

13. The consent of the data subject means any voluntary, explicit, informed and unequivocal declaration of will by the data subject, by which he expresses his consent to the processing of personal data relating to him by means of a statement or a clear affirmative action.

14. Special types of personal data are personal data revealing racial or ethnic origin, political opinion, religious or philosophical belief or trade union membership, and the processing of genetic data, biometric data for the purposes of unique identification of an individual, data related to health or data related to an individual's sex life or sexual orientation.

Article 3

A description of the collections of personal data managed by the company is kept in the record of processing activities in accordance with the provisions of Article 35 of the GDPR.

Records of processing activities are not kept.

Employees who process personal data must be familiar with the records of personal data processing activities, and access to the records of personal data collections must also be made available to anyone who requests it.

The following information is entered in the records of processing activities: title or name and contact details of the controller, name of the personal data collection, legal basis, purpose of processing, categories of individuals, types of personal data, internal and external users,

retention (deletion) periods , methods of securing personal data data , the responsible person of the collection and the information support of the collection .

Employees who process personal data must be familiar with the records of personal data processing activities, and access to the records of processing activities must be made available only to those employees who need personal data for the purposes for which they are processed.

At its request, the security officer allows the supervisory authority to view the records of processing activities.

II. LEGAL DATA PROCESSING

Article 4

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

Article 5

When it is possible that the type of processing, especially with the use of new technologies, taking into account the nature, scope, circumstances and purposes of processing, could cause a high risk to the rights and freedoms of individuals, the controller shall carry out an assessment of the impact of the intended processing actions on the protection of personal data before processing. Several similar processing actions, which are not related to each other, may be considered in one assessment.

When carrying out an impact assessment in relation to data protection, the manager asks the company director for an opinion.

The assessment covers at least:

(a) a systematic description of the intended processing actions and purposes of the processing, when appropriate, as well as the legitimate interests pursued by the controller;

(b) assessment of the necessity and proportionality of processing actions in relation to their purpose;

(d) measures to address the hazard.

I II. SECURITY OF PREMISES AND COMPUTER EQUIPMENT AND OTHER HOLDERS OF PERSONAL DATA

Article 5

Premises in which personal data carriers, hardware and software are located (secured premises) must be protected by organizational and physical and/or technical measures that prevent unauthorized persons from accessing the data.

Access is only possible during regular working hours, and outside these hours only with the permission of the head of the organizational unit.

Holders of personal data may not leave the business premises of LexEU unless this is absolutely necessary for the performance of work tasks in the field (e.g. meeting of owners, handover of documentation with a new manager, etc.) or for the transfer of holders of personal data from one business unit to another. In the case of transfer of carriers with personal data for the purposes specified in this paragraph, the individual employee must indicate in the relevant personal data records which carriers or documents were taken out, for what purpose and when they were returned.

Article 6

The keys to the secured premises are used and kept by LexEU. The keys are not left in the lock in the door from the outside. Outside of working hours, cabinets and desks with personal data carriers must be locked, computers and other hardware must be turned off and physically or software locked. Protected areas must not remain unattended, or they must be locked in the absence of the workers supervising them.

Holders of personal data located outside secured premises (corridors, common areas) must be permanently locked.

Special types of personal footwear must not be kept outside of secured areas.

Article 7

In rooms intended for dealing with customers, data carriers and computer displays must be installed in such a way that customers cannot see them. Employees must not leave personal data carriers on their desks in the presence of persons who do not have the right to view them.

In the event of an employee leaving the premises referred to in the previous paragraph, the computer displays must be locked so that an unauthorized person cannot access the data therein.

Article 8

Maintenance and repairs of computer hardware and other equipment is only permitted with the knowledge of an authorized person, and it can only be carried out by authorized services and maintenance personnel who have a LeksEU license an appropriate contract has been concluded.

9 . Article

Maintainers of premises, hardware and software, visitors and business partners may move in the premises referred to in the first paragraph of Article 5 of these regulations only with the knowledge of an authorized person. Employees, such as cleaners, security guards, etc., can only move outside of working hours in those protected areas where access to personal data is prevented (data carriers are stored in locked cabinets and desks, computers and other hardware are switched off or otherwise physically or software locked).

IV. PROTECTION OF SYSTEM AND APPLICATION SOFTWARE COMPUTER EQUIPMENT AND DATA PROCESSED WITH COMPUTER EQUIPMENT

Article 10

Access to the software must be protected in such a way that it allows access only to previously specified employees or legal or natural persons who perform the agreed services in accordance with the contract.

Article 11

Repairing, changing and supplementing the system and application software is only permitted based on the approval of an authorized person, and it can only be carried out by authorized services and organizations and individuals who have concluded an appropriate contract with LixEU, in which it is mandatory to determine the conditions and measures for ensuring the protection of personal data and their insurance also applies to external parties who maintain hardware and software and manufacture and install new hardware or software.

Contractors must properly document changes and additions to system and application software and hand over such a document to an authorized person after the work has been completed.

Article 12

The content of the disks of the network server and local workstations, where personal data is located, is regularly tested, evaluated and the effectiveness of technical and organizational measures is evaluated. The presence of possible computer viruses is constantly checked .

All personal data and software that are intended for use in a computer information system and arrive at Lex EU on computer data transfer media or via telecommunications channels must be checked for the presence of computer viruses before use.

The person responsible for the operation of the computer information system is responsible for the obligations from this article

1 Article 3

Employees may not install software without the knowledge of the person responsible for the operation of the computer information system. They must also not carry away the leXEU software . without the approval of the head of the organizational unit and the knowledge of the person in charge of the operation of the computer information system.

Article 14

Access to data through the application software is protected by a password system for authorization and identification of users of programs and data, and the password system must also allow the possibility of subsequently determining when individual personal data was entered into the database, used or otherwise processed and who it is did.

The authorized person determines the regime of assigning storage and changing passwords.

Article 15

All passwords and procedures used for entering and administering the network of personal computers (supervisory or control passwords), administering e-mail and administering application programs are kept in sealed envelopes and are protected against access by unauthorized persons. They should only be used in exceptional circumstances or emergencies. Any use of the contents of the sealed envelopes shall be documented. After each such use, a new password content is determined.

Article 16

For the needs of restoring the computer system in the event of malfunctions and other exceptional situations, regular copies of the content of the network server and local stations, if the data is located there, are guaranteed.

These copies are kept in designated locations.

V. SERVICES PROVIDED BY EXTERNAL LEGAL OR INDIVIDUAL PERSONS

Article 17

A written contract is concluded with any external legal or physical person who performs individual tasks related to the collection, processing, storage or forwarding of personal data and is registered to perform such activity (processor). Such a contract must specify the content and duration of processing, the nature and purpose of processing, the type of personal data, the categories of individuals to whom personal data relate, the rights and obligations of the controller, and the mandatory conditions and measures to ensure the protection of personal data and their insurance.

External legal or natural persons may provide personal data processing services only within the framework of the documented instructions of the controller, they may not process or otherwise use the data for any other purpose.

Authorized legal or natural person who for LexEU performs the agreed services outside the operator's premises, it must have at least as strict a method of protecting personal data as provided for in these regulations.

VI. ACCEPTANCE AND TRANSFER OF PERSONAL DATA

Article 18

The employee who is in charge of receiving and recording the mail must hand over the mail with personal data directly to the individual, or to the department to which the mail is addressed, to the person responsible for the individual collection of personal data.

The employee who is in charge of receiving and recording mail opens and inspects all mail items and items that arrive at the company in another way they are brought by customers or couriers, except for shipments from the third and fourth paragraphs of this article.

The employee who is in charge of receiving and recording mail does not open those shipments that are addressed to another authority or organization and are delivered by mistake, as well as shipments that are marked as personal data or that it follows from the markings on the envelope that they refer to competition or tender.

The employee who is in charge of receiving and recording mail may not open shipments addressed to the employee, on which it is stated on the envelope that they are to be served personally to the addressee, as well as shipments on which the personal name of the employee is first stated without indicating his official position and only then the title Lex EU .

Article 19

Personal data may only be transmitted by information, telecommunication and other means when procedures and measures are implemented to prevent unauthorized persons from misappropriating or destroying data and from unauthorized access to their content.

Special types of personal data are sent to addressees in sealed envelopes against a signature in the delivery book or by delivery note.

The envelope in which personal data is transmitted must be made 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 with ordinary light. Also, the envelope must ensure that the opening of the envelope and familiarization with its contents cannot be done without a visible trace of the opening of the envelope.

Article 20

The processing of a special type of personal data must be specially marked and secured.
The data from the previous paragraph may be transmitted via telecommunications networks only if they are specially secured with cryptographic methods and electronic signatures in such a way that the unreadability of the data during their transmission is ensured.

Article 21

Personal data are provided only to those users who prove themselves to be on the appropriate legal basis or with a written request or consent of the individual to whom the data relates, in which case the application must be accompanied by a written request or consent of the individual to whom the data relates.

Unless another law provides otherwise, the request for the provision of personal data contains the following information (Article 41 ZVOP-2):

- information about the applicant (for a natural person: personal name, address of permanent or temporary residence; for a self-employed individual, an individual carrying out an activity independently, and for a legal entity: name or company and address or registered office and registration number) and the signature of the applicant or authorized persons;
- the legal basis for obtaining the requested personal data;
- the purpose of processing personal data, or the reasons that demonstrate the necessity and suitability of personal data to achieve the purpose of acquisition;
- the subject and number or other identification of the matter in connection with which personal data is required, as well as the indication of the authority or other entity handling the matter;
- the types of personal data to be provided to him;
  the form and method of obtaining the required personal data.

Unless otherwise stipulated by another law, the administrator shall provide the requester with the requested personal data no later than 15 days after receiving the complete request, or shall notify the requester in writing within this period of the reasons for not providing the requested personal data. The controller and the requester can agree on an extension of the deadline from the previous sentence.

If the controller does not comply with the previous paragraph, the request is considered rejected.

The authorized person for data protection has at least the following tasks:

(a) informing the controller or processor and the employees who carry out the processing and advising them of their obligations in accordance with this Regulation and other provisions of Union or Member State law on data protection;

(b) monitoring compliance with this Regulation, other provisions of Union law or Member State law on data protection and policies of the controller or processor in relation to the protection of personal data, including the assignment of tasks, awareness and training of personnel involved in processing actions, and thereby related audits;

(c) counseling.

For each transmission of personal data, the operator provides the possibility of later ascertaining which personal data were transmitted, to whom, when and on which legal basis, for which purpose or for which reasons or for the needs of which procedure .

The manager keeps the information from the previous paragraph for two years, unless another law specifies a different deadline for the transmission of individual types of data.

Original documents are never provided, except in the case of a written court order. The original document must be replaced by a copy during the absence.

VII. DATA DELETE

Article 22

Personal data are stored only for as long as necessary to achieve the purpose, after the fulfillment of the processing purpose, personal data are deleted, destroyed, blocked or anonymized, if they are not defined as archive material on the basis of the law governing archival material, or if the law for individual does not specify the type of personal data otherwise.

The terms by which personal data are deleted from the database can be seen from the records of processing activities.

Article 23

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

Data on classic media is 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.

VIII. ACTION IN THE CASE OF SUSPECTED UNAUTHORIZED ACCESS

Article 24

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

In the event of a breach of personal data protection, 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 it is unlikely that the rights and freedoms of individuals would be threatened by the breach of personal data protection. When the official notification to the supervisory authority is not given within 72 hours, it shall be accompanied by a statement of the reasons for the delay.

IX. RESPONSIBILITY FOR THE IMPLEMENTATION OF SECURITY MEASURES AND PROCEDURES

Article 25

Heads of organizational units and authorized persons are responsible for the implementation of procedures and measures for securing personal data.

Article 26

Everyone who processes personal data is obliged to implement the prescribed procedures and measures for securing data and to protect the data that they learned about or were aware of while performing their work. The obligation to protect data does not end with the termination of the employment or contractual relationship.

Before starting work at a workplace where personal data is processed, the employee must sign a special declaration obliging him to protect personal data.

It must be clear from the signed declaration that the signatory is familiar with the provisions of this rulebook and the provisions of the General Data Protection Regulation and ZVOP-2, and the declaration must also contain instructions on the consequences of the violation.

Article 27

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

X. FINAL PROVISIONS:

Article 28

On the day this policy comes into force, the policy ceases to be valid.

Article 29

This policy comes into effect on __ _____ _ day after __ _____ _____

Legal representative, e.g. director
Name and surname and signature

In __place and date