General Terms of Use and Rules of Conduct in SRCE Data Centres

1. Annex to the Ordinance on Data Centre Management

General Terms of Use and Rules of Conduct in Data Centres

I. Introduction

General Terms of Use and Rules of Conduct in Data Centres (hereinafter referred to as: General Terms) regulate the use of data centres in order to enable the safety and protection of authorized persons and the User's equipment in the premises of data centres.

Users of data centres are SRCE and Partners in accordance with this Ordinance and agreements on the management and use of data centres.

Users of data centres are also legal entities with whom the housing agreement was concluded.

General Terms apply to Users and authorized persons of Users who have been granted the right of access (hereinafter referred to as: authorized persons).

II. General Terms

Premises of data centres are intended for the collocation of equipment, and authorized persons stay in them only when physical access is required for the purpose of entering, installing, controlling, adjusting and maintaining the User's equipment. When performing their duties, authorized persons are obliged to comply with security procedures in order to protect the data centres and ensure the optimal functioning of the data centres.

Authorized persons must not, by their behaviour or their activities, interfere with employees, associates, other parties and visitors in the activities for which they stay in the building where the data centre premises are located.

While staying in the premises of the data centre, the following is prohibited:

- Access premises for which you do not have a permit, perform activities and bring in equipment for which no permit has been issued
- Smoking, eating and drinking
- Wear dirty clothes and shoes or bring in dirty tools and equipment
- Sawing, drilling, welding or use open flame, i.e. performing any actions that result in the generation of dust, high temperature, sparks or smoke
- Perform mechanical work inside the computer hall (if necessary, it can be done in the hall only with the permit of the operational manager of the data centre)
- Bring in weapons of any kind; corrosive, caustic, aggressive, flammable and explosive substances
- Bring in and store other flammable materials (wood, cardboard, plastic materials, flammable liquids and solvents), unless a permit for this is obtained by the manager of the data centres
- Bring in electronic equipment, especially equipment for recording photos, video and sound recordings (except mobile phones, the use of which is allowed, but without the use of a camera)
- Bring in equipment for wireless communication and data transmission (except personal laptops)
- Turn on and off any equipment other than the User's equipment
- Move, bring in and take out equipment, cut and move any cables except the equipment and cables of the User
- Open and close any valves
- Make changes, adaptations or improvements in the premises and place boards or advertisements without the prior written consent of the data centre manager
- Perform actions that could cause damage to equipment in the data centre.

Authorized persons are expected to be familiar with the ANSI/TIA-942 standard in the part related to work in computer rooms.

After completing work in the premises of the data centre, authorized persons are obliged to return the premises to their original state, i.e. remove all material, equipment and tools that they brought for the purpose of performing work, as well as all waste material, impurities, etc. that arise during the performance of the work.

III. Physical protection and security

Data centres are facilities with access control. Access to data centres and related facilities is permitted only to authorized persons.

Authorized persons have limited access to data centre premises depending on the level of security assigned to them.

Physical protection includes the presence of security guards, entrance procedures for entry and exit, allocation of cards and keys, an automated system for granting access rights and a procedure for submitting requests for granting access rights.

Security cameras (video surveillance) monitor all areas of data centres, including lobbies, common and technical areas, computer halls and the environment.

Persons who fail to comply with data centre rules shall bear all the legal consequences of such behaviour. Any action that affects the proper functioning of data centre security systems is strictly prohibited.

Data centre authorized persons can access any part of the data centres at any time for security reasons.

Physical protection personnel of the facility where the data centre is located, i.e. the representative of the data centre, has the right to interrupt the activity and stay of authorized persons in the data centres during their stay in the premises of the data centre if they believe that there has been a violation of security rules, i.e. exceeding the authorizations issued.

In case of smoke detectors or emergency alarms, authorized persons are obliged to leave the data centres and follow the instructions they receive from the data centre representative.

IV. Protection of personal data collected by video surveillance

Collection of personal data through video surveillance represents the legitimate interest of SRCE for the purpose of ensuring the protection of persons and equipment of SRCE and Users in the premises of the data centres.

Personal data collected using the video surveillance system shall not be used for other purposes.

SRCE shall keep video surveillance recordings for 30 days from the day they were created.

In the event that a review of the video surveillance recording has established that there has been damage to the property of SRCE or the entry into SRCE premises by unauthorized persons, and in any other case where an incident has been established that can be considered risky for the protection of property and people, the video surveillance system recordings shall be kept until the end of a judicial, administrative, arbitration or other procedure in which they can be used as evidence to establish the facts related to the incident that led to the implementation of the procedure.

Persons whose data is collected through video surveillance shall, under the terms of the General Data Protection Regulation, have the right to access personal data, the right to erasure (right to be forgotten), the right to limit processing, the right to object to processing and the right to correction.

Data Protection Officer's contact details: zop@srce.hr Additional information is published on SRCE website – www.srce.unizg.hr/kontakt.

Objections to the processing of personal data are submitted to the Agency for the Protection of Personal Data.

V. Entry and exit from data centres

All authorized persons entering data centres shall:

- At the request of the security guard, provide a valid ID with a photo for inspection
- Be authorized to enter the data centre
- Log in and log out when entering the data centre
- Before leaving the data centre, hand over access cards, keys, tools or other things owned by the data centres.

VI. Right of entry to data centres

Users shall:

- Submit and update the list of persons authorized to enter the data centre
- Announce and receive approval for the arrival of authorized persons in a timely manner via electronic mail
- Announce and receive approval for the arrival of third-party Users accompanied by an authorized person in a timely manner via electronic mail.

Authorized persons shall be granted access only to the premises where they perform their work.

VII Procedure for bringing in the User's equipment

Upon arrival of the equipment, initial configuration or unpacking the equipment for the purpose of removing the packaging, the aforementioned actions must be performed in the unpacking area. After completing these actions, the equipment can be brought into the data centre premises. The unpacking area cannot be used as a storage area.

After bringing in the equipment into the data centre premises, the User shall remove all packaging from the unpacking area and the data centre area.

The User undertakes to request and obtain SRCE approval for each entry and collocation of equipment in data centres and to comply with the prescribed security procedures during entry in order to protect the data centres and prevent possible operational difficulties.

Zagreb, 27 May 2022