

## Data Protection Notice

### Agency Offices

(December 2018)

This Data Protection Notice is provided to you in order to explain the policy of the Agency for the Cooperation of Energy Regulators ("the **Agency**") regarding your privacy, as well as how your personal information is handled when accessing and using facilities within the Agency's offices, located at the TR3 Building, Trg republike 3, 1000 Ljubljana, Slovenia ("**Offices**").

### Who is responsible for my personal information?

The Agency is the data controller regarding all personal data processing carried out in relation to persons accessing and using facilities within the Offices.

To get in touch with the Agency's Data Protection Officer, please contact: [dpo@acer.europa.eu](mailto:dpo@acer.europa.eu).

### What personal information of mine is being collected?

When you visit the Offices, or use certain facilities within the Offices, the Agency may collect and process information related to you (as an individual), which, either by itself, or together with other information to which the Agency has access, allows you to be identified.

This information may be classified as "**Personal Data**".

Personal Data which may be processed by the Agency in this context are as follows:

#### (a) **Access Control Data**

Access cards will be issued to every person accessing the Offices (including staff members, trainees, external experts or visitors), in order to allow those persons to access different rooms and offices belonging to the Agency within different floors of the TR3 Building. These cards are needed to operate doors with proximity card readers within the Offices.

In order to provide you with an access card, the Agency collects Personal Data related to you, such as your name and organisation (as well as your department within the Agency, where applicable). Furthermore, the Agency keeps records of the locations accessed and times at which those locations were accessed with the issued access cards.

Additionally, the Agency relies on a key handler system, which allows the Agency to identify access cards used in order to obtain access to keys related to specific doors within the Agency's offices. This system not only identifies which access card was used to retrieve a given key, but also tracks any unauthorised attempts to take such keys with force (identifying, in these cases, the last access card read).

(b) **Closed-Circuit Television (CCTV) Footage**

A CCTV system is installed within the TR3 Building, covering all entrances to the Offices. This system works based on a proximity sensor, records footage captured near those entrances where movement is sensed – as such, whenever you enter or exit the Offices, your likeness is recorded. Where it is possible to identify you as an individual, via this footage or in combination with other information, this footage is considered as Personal Data relating to you.

All such footage are stored on Agency servers, protected by physical locks and a PIN code for access.

(c) **Wi-Fi Data**

The Agency offers access to free Wi-Fi to its visitors and personnel. When accessing the Wi-Fi, as an inherent part of its operation, the Agency collects information related to the device you use, such as its IP address and MAC address.

(d) **Special categories of Personal Data**

Special categories of Personal Data include information revealing your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data related to you or data concerning your health, sex life or sexual orientation. Additionally, for the purposes of this Data Protection Notice, Personal Data relating to offences, criminal convictions or security measures will also be considered as special categories of Personal Data.

Footage collected from the CCTV system might potentially allow to infer special categories of Personal Data related to you (depending on the actions recorded). The Agency only processes any Personal Data collected via the CCTV system where those Personal Data are necessary, adequate and relevant for physical security purposes (e.g., prevention and investigation of security incidents).

## Why is the Agency using these Personal Data?

The Agency uses the Personal Data mentioned above for one or more of the following purposes:

(a) **Physical Security**

To ensure that only authorised persons have access to the Offices, and that the Agency is able to monitor and track which access cards have been used at given locations and times (in the event this is necessary for audits or investigations). Additionally, to safeguard the physical security of the Offices, as well as of the Agency's personnel and visitors, by preventing and investigating potential security incidents.

- It is mandatory to provide Personal Data to the Agency for this purpose, without which you will not be granted access to the Offices.

(b) **Wi-Fi Access**

To allow the operation of the Agency's Wi-Fi network, for the benefit of visitors and personnel.

(c) **Compliance**

For compliance with laws which impose upon the Agency the collection and/or further processing of certain kinds of Personal Data.

- When you provide any Personal Data to the Agency, the Agency must process it in accordance with the applicable law, which may include retaining and reporting your Personal Data to official authorities for compliance with its legal obligations.

All Personal Data processed by the Agency may further be included in periodic backups carried out to ensure the availability of information stored on the Agency's IT systems, and may further be processed to ensure the appropriate handling of security incidents related to those systems, as well as the Agency's compliance with its legal obligations regarding the processing of Personal Data (e.g., related to management of personal data breaches).

## Why can the Agency use these Personal Data?

The legal bases which the Agency relies on to process this Personal Data, according to the purposes identified above, are the following:

(a) **Physical Security**

Processing for this purpose is necessary to safeguard physical security of visitors and personnel within the Offices which, in turn, is necessary for the proper management and functioning of the Agency.

(b) **Wi-Fi Access**

Processing for this purpose is necessary to provide a service requested by persons accessing the Agency's Wi-Fi network (as it is an inherent part of the operation of this network).

(c) **Compliance**

Processing for this purpose is necessary for the Agency to comply with its legal obligations.

The inclusion of all Personal Data stored by the Agency in its IT systems in periodic backups, as well as all processing carried out to ensure the appropriate handling of security incidents related to those systems, is deemed necessary in order to ensure the proper management and functioning of the Agency and, as such, necessary to perform a task in the public interest.

## Who can see your Personal Data, and who will they be shared with?

Your Personal Data may be shared with the following list of persons / entities ("**Recipients**"):

- **CEEREF Nalozbe d.o.o.**, Dunajska cesta 9, Ljubljana, Slovenia – the owner of the TR3 Building, which provides and operates the access control system mentioned ("**TR3 Building Owner**");
- Companies, entities or professional associations engaged by the Agency, including other Union institutions or bodies, in order to provide services related to maintenance of the access control, CCTV and Wi-Fi systems, as well as technical maintenance / assistance and operational security of systems used to store Personal Data processed in connection with the purposes described in this Notice, which typically act as data processors on behalf of the Agency, and have access to Personal Data only to the extent strictly required for them to provide those services;
- Persons authorised by the Agency to process Personal Data needed to carry out activities strictly related to the purposes described above, who have undertaken an obligation of confidentiality or are subject to an appropriate legal obligation of confidentiality (e.g., staff members of the Agency);
- Public entities, bodies or authorities, including other Union institutions or bodies, to which your Personal Data may be disclosed, in accordance with Union or Member State law, or with binding orders from those entities, bodies or authorities.

The Agency will not transfer your Personal Data outside of the EU.

For more information on transfers of Personal Data carried out by the Agency for these purposes, please contact the Agency's Data Protection Officer, at: [dpo@acer.europa.eu](mailto:dpo@acer.europa.eu).

## How long do we keep your data?

The retention periods applicable to Personal Data handled by the Agency, for the purposes described in this Data Protection Notice, are as follows:

### (a) **Physical Security**

Personal Data related to the use of access cards are stored by TR3 Building Owner, and accessible to the Agency upon request, for the period defined by applicable Slovenian law.

CCTV footage is retained by the Agency for 45 days.

Information retained in the Agency's key handler system is logged for 1 year.

### (b) **Wi-Fi Access**

Personal Data processed for **Wi-Fi Access** are stored by the Agency for as long as a user remains connected to the Wi-Fi network, or for up to 1 day.

### (c) **Compliance**

Personal Data processed for **Compliance** are kept by the Agency for the period required by the specific legal obligation or by the applicable Union or Member State law.

Please note that, in any case, the Agency may continue to store Personal Data for a longer period, as may be necessary for internal auditing and security purposes (including within periodic backups carried out) and, in general, to protect the Agency's interests related to potential liability related to this processing.

For more information on the applicable retention periods, please contact the Agency's Data Protection Officer, at: [dpo@acer.europa.eu](mailto:dpo@acer.europa.eu).

## What are my rights? How can I exercise them?

As a data subject, you are entitled, in general, to exercise the following rights before the Agency:

- Access your Personal Data being processed by the Agency (and/or obtain a copy of those Personal Data), as well as information on the processing of your Personal Data;
- Correct or update your Personal Data being processed by the Agency, where it may be inaccurate or incomplete;
- Request the erasure of your Personal Data being processed by the Agency, where you feel that the processing is unnecessary or otherwise unlawful;
- Request the blocking of your Personal Data, where you feel that the Personal Data processed is inaccurate, unnecessary or unlawfully processed, or where you have objected to the processing;
- Exercise your right to portability: the right to obtain a copy of your Personal Data provided to the Agency, in a structured, commonly-used and machine-readable format, as well as the transmission of that Personal Data to another data controller.

You may also have a right to **object to the processing of your Personal Data**, based on relevant grounds related to your particular situation, which you believe must prevent the Agency from processing your Personal Data for a given purpose. This right may apply whenever the Agency relies on the need to perform a task in the public interest as the legal basis for a given processing purpose, e.g., **Physical Security** and others (see above – [Why can the Agency use these Personal Data?](#))

To exercise any of the abovementioned rights, you may send a written request to the Agency, at: [dpo@acer.europa.eu](mailto:dpo@acer.europa.eu).

Please note that the above rights may not apply, or may not apply in full, as there may be applicable legal exemptions or restrictions to those rights. This will be assessed by the Agency on a case-by-case basis; if such an exemption or restriction is found to be applicable, you will be informed of the Agency's main reasoning for this.

In any case, please note that, as a data subject, you are entitled to file a complaint with the European Data Protection Supervisor, if you believe that the processing of your Personal Data carried out by the Agency is unlawful. You will suffer no prejudice on account of any such complaints lodged.