Processing of personal data at CESNET association

In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as "GDPR"), we hereby inform you about how we process personal data when providing CESNET e-infrastructure

Who is the personal data controller and who is the data subject:

The personal data controller within the meaning of the GDPR is CESNET, an interest group of legal entities (hereinafter referred to as the"CESNET association"). The controller is responsible for the proper and lawful processing of personal data.

Contact details for the CESNET association and its data protection officer can be found here: https://www.cesnet.cz/kontakty.

The CESNET e-infrastructure, operated by the CESNET association, is a large research infrastructure within the meaning of Act No. 130/2002 Coll., on the support of research, experimental development, and innovation, and provides services to organizations that meet the Conditions for Access to the CESNET e-infrastructure. By accessing the CESNET e-infrastructure, an organization (and through it, individual natural persons – for example, employees and students, i.e., data subjects as defined by the GDPR) access to a unique set of services in the field of information and communication technologies: premium high-speed access to the Internet and to partner networks for science, research, and education around the world, as well as environments for data storage, high-performance computing, collaboration support, security, identity management, and other services.

Processing of Personal Data at e-INFRA CZ:

The CESNET e-infrastructure is part of a unique e-infrastructure for research, development, and innovation in the Czech Republic

called e-INFRA CZ, which consists of:

- the CESNET e-infrastructure, operated by CESNET, an association of legal entities, ID No.: 63839172;
- CERIT Scientific Cloud, operated by Masaryk University, ID No.: 00216224; and
- IT4Innovations National Supercomputing Center, operated by the VŠB – Technical University of Ostrava, ID No.: 61989100.

One of the goals of e-INFRA CZ is to integrate its individual components so that users have unified access to e-INFRA CZ services and receive consistent user support when using these services. e-INFRA CZ services are available to users who hold e-INFRA CZ user status in accordance with the Terms and Conditions for Access to the e-INFRA CZ Infrastructure.

For the purposes of operating and fulfilling the objectives of e-INFRA CZ, selected personal data of CESNET e-infrastructure users, where necessary, are processed jointly by all e-INFRA CZ operators under the joint controller arrangement as defined in Article 26 of the GDPR. Joint processing of personal data will not apply to users for whom this is legally prohibited (see Article II (3) of the Terms and Conditions for Access to the e-INFRA CZ Infrastructure).

Detailed information about the joint processing of personal data at e-INFRA CZ can be found here: www.e-infra.cz/zpracovani-osobnich-udaju.

Purposes and Legal Basis for the Processing of Personal Data in the CESNET e-Infrastructure:

We process only the data necessary for providing services and user support, for fulfilling obligations arising from legislative regulations, and for meeting other obligations (e.g., the terms and conditions of support providers within projects). We process the data of users of our services (current and former), and to a limited extent, potential users who have expressed interest in the services and with whom communication regarding access to the services has been established. Without providing the personal data required to ensure the operation of the CESNET e-infrastructure, it is not possible to use its services.

When providing CESNET e-infrastructure services, we process your basic personal and contact information, operational and usage data, data from our communications with you, and any other relevant data, ensuring that the scope of such data is appropriate and limited to what is necessary for the purpose for which we collect and process your personal data.

Purposes and Legal Basis for the Processing of Personal Data in the CESNET e-Infrastructure:

Unless otherwise specified, **we process the following categories of personal data based** on CESNET's legitimate interest in providing services that will be:

- of appropriate quality, which is why we monitor service operations and conduct evaluations;
- secure, which is why we monitor the network and applications and respond immediately to detected threats;
- provided in accordance with the rules of grant providers, which is why we adjust the rules for using the services and retain records of them to the required extent;
- in cooperation with national and international organizations and infrastructures with a similar focus.

Access to the Service

To access services that require authentication and authorization for quality and security purposes, users must create a user identity in one of the IdM systems we operate. To provide these services, we need to know your basic identification and contact details, as well as information about your home organization. This information is provided to us when you first access the CESNET e-infrastructure. Furthermore, for the purpose of performing authorization and authentication, we record various internal identifiers and information about user permissions.

When accessing CESNET e-infrastructure services that do not require authentication and authorization, personal data such as the IP address (as well as other identifiers enabling the tracing of the source and destination of communication) and other unique identifiers used by individual services are processed.

Ensuring the Service's Own Operation

To ensure your access to CESNET's e-infrastructure services, provide high-quality services, develop them, resolve operational and security issues, and, among other things, protect your personal data, we perform analyze and process system and service operation records (logs), operational and location data from operational and security monitoring, and optimize the execution of individual tasks and the service itself.

Monitoring and Security

To ensure operational stability and service security, to protect users and their data, and to address cybersecurity events and incidents, we process information from network traffic and from users' access to individual services (so-called operational and location data, logs). This information may include, for example, technical identifiers of the traffic generated, information about the user identity requesting access to the service, the result of the authentication process, or timestamps of access or attempted access.

We process the above information not only based on our legitimate interest but also to comply with legal obligations. These legal obligations arise, for example, from Act No. 127/2005 Coll., on Electronic Communications, and from Act No. 264/2025 Coll., on Cybersecurity, which establish obligations regarding the retention of operational and location data and the detection and reporting of cybersecurity incidents.

Statistics

To ensure the sustainable operation of the CESNET e-infrastructure and its services, as well as to support development, security, and service quality improvement, and to fulfill reporting obligations to grant providers and members, we process primary data using statistical methods. This data typically includes the utilization rate of the CESNET e-infrastructure, the manner in which the CESNET e-infrastructure is used, service

utilization, the number of detected and reported operational and security issues, the types and severity of operational and security issues, etc.

Communication

We process information from communications, meetings, consultations, and phone calls (in the form of notes and recordings), as well as from email communications regarding operational or security issues (within ticketing systems), including the resolution of complaints and service requests, and information from communications related to securing access to the service, etc. Thanks to this information, we can improve our services, internal processes, and user support. We also process feedback, comments, suggestions, and the results of non-anonymous surveys as personal data.

Retention period for personal data:

- When processing your personal data, we adhere to the principle of data minimization. We retain only the data necessary to provide CESNET e-infrastructure services and to safeguard your rights.
- The actual processing of personal data begins upon your first use of the CESNET e-infrastructure service, and personal data—including first name, last name, email address, phone number, name of home organization, and user identity in an external IdM system (e.g., EPPN)—is retained in non-anonymized form for the entire duration of your use of the CESNET e-infrastructure service.
- Personal data: first name, last name, email address, name of home organization, user identity in an external IdM system (e.g., EPPN), user identity created for the CESNET e-infrastructure, and the unique user identifier for the CESNET e-infrastructure are retained even after the termination of use of CESNET e-infrastructure services for security reasons (primarily to prevent duplicate user account identities) and for the purpose of reporting on the use of CESNET e-infrastructure resources. The administrator shall establish technical and organizational conditions for the protection of personal data to ensure their integrity and confidentiality.
- ē Personal data in the form of operational and location data (so-called logs), such as IP addresses (as well as other identifiers that allow the source and destination of communication to be traced) and other unique identifiers used by individual services of the -infrastructure are stored for a period of 18 months and then deleted, unless otherwise specified in the terms of service for a specific service.
- Personal data appearing in security incident reports, along with the entire course of the security incident resolution—i.e., including communication with the person responsible for resolution (which typically contains the following data: first name, last name, email, and name of home organization)—is retained in its original form

and is not deleted. The same applies to reports and resolutions of operational issues.

- We retain information from communication infrastructure monitoring—i.e., information obtained by collecting data from active network elements and information about IP flows—in full quality (without loss of informational value) for 6 months, and in summarized form (with loss of informational value) as statistical data for 5 years. We retain personal data related to information on the use of CESNET e-infrastructure resources for as long as it is necessary for the operation and improvement of the service, or, in the case of projects, for the period specified by individual providers of project-specific support, but for at least 5 years after the completion of the projects.

Recipients of Personal Data

The CESNET Association discloses personal data to other entities only when necessary. Where possible (i.e., provided it does not conflict with the purposes of disclosure set forth below), we disclose only anonymized data.

Disclosure Based on Legal Requirements

Under the Cybersecurity Act, the CESNET Association is required to report detected cybersecurity incidents. Reports of cybersecurity incidents may contain IP addresses related to the reported incident, to a lesser extent other technical identifiers, and in very limited cases, the information may be of such a nature that it can be linked to a data subject.

Under the Electronic Communications Act, CESNET is required to transfer traffic and location data to designated entities in specified cases. CESNET transmits this data in the case of services that fall under this Act.

We are also required to provide network traffic logs, which may contain identifiers such as IP addresses, MAC addresses, or other technical identifiers, to law enforcement authorities upon request.

Disclosure Based on Legitimate Interest

Personal data in the form of operational and location data, as well as other unique identifiers used by individual CESNET e-infrastructure services, may be disclosed to network and service administrators from organizations connected to the CESNET e-infrastructure and to members of security teams as part of the process of resolving operational issues and security incidents.

The Association is a member of national and international security infrastructures (Fenix, TF-CSIRT, CSIRT.CZ Working Group), where an informal condition of participation is the sharing of security-related experience and information, which

includes sharing information about detected security events, anomalies, and vulnerabilities.

Personal data in the form of statistically processed data on the use of CESNET e-infrastructure resources is shared with CESNET association members and providers of targeted support.

Data Subject Rights:

With regard to personal data processed within the CESNET e-infrastructure, you may exercise the following rights with the CESNET Association:

- the right to information and access to personal data (Article 15 of the GDPR),
- the right to rectification (Article 16 of the GDPR),
- the right to erasure (Article 17 of the GDPR),
- the right to restriction of processing (Article 18 of the GDPR),
- the right to object (Article 21 of the GDPR),
- the right to lodge a complaint with the Office for Personal Data Protection – you may contact the Office for Personal Data Protection at any time with a request, suggestion, or complaint at pplk. Sochora 27, 170 00 Prague 7.

The above information regarding the processing of personal data is effective as of November 12, 2021.