PRIVACY POLICY

1. INTRODUCTION

Croatian Transmission System Operator Plc (hereinafter referred to as "HOPS") pays great attention to the protection and processing of personal data. The purpose of this Privacy Policy (hereinafter: "Policy") is to provide information on all relevant features of personal data collection, processing and storage.

Protection of personal data of all individuals, in all procedures that we carry out every day in order to fulfill our business and legal obligations, is one of the fundamental policies and obligations that we adhere to in our business.

Through a systematic approach to the management of personal data protection, we want to create safe environment for all individuals that will ensure privacy and fundamental freedoms and rights in relation to personal data for our employees and clients, partners and suppliers.

Implementation of the principles and guidelines from this policy throughout HOPS is mandatory over the entire scope of business operations in which personal data of respondents are used and processed.

2. PROCESSING MANAGER

The manager of personal data processing is the Croatian Transmission System Operator Plc

- Kupska 4, Zagreb
- OIB: 13148821633
- e-mail:kontakt@hops.hr
- Telephone: +385 1 45 45 111

You can find more detailed information about the Croatian Transmission System Operator Plc at https://www.hops.hr/

3. INFORMATION ABOUT THE DATA PROTECTION OFFICER

For all questions regarding personal data, you can contact our data protection officer via e-mail (SzZP@hops.hr) or by telephone (+385 1 45 45 111). In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data and on repealing Directive 95/46/EC (hereinafter referred to as the GDPR Regulation), we will provide you with information about the actions we have taken at your request, no later than one month after receiving the request. If necessary, this deadline can be extended by additional two months, taking into account the complexity and number of requests received.

We will notify you of any extension within one month of receiving the request, stating the reasons for the delay.

4. COLLECTION AND PROCESSING OF PERSONAL DATA

In performing the tasks for which we are registered as a company, we collect and process different categories of personal data for the purpose of:

- Fulfilling contractual obligations towards our clients, partners and suppliers
- Fulfilling our legal obligations
- Communication with the public.

4.1. Workers

The processing is performed exclusively on the basis of legal obligations related to labor relations. All data about workers are stored and processed in the territory of the Republic of Croatia, on the official premises of HOPS or with contractual suppliers (processors), in compliance with the principles of the GDPR Regulation.

4.2. Job candidates

Processing of personal data is carried out periodically, based on the Decisions of the HOPS Management Board and HOPS by-laws related to employment. All processing is carried out on the premises of HOPS on the equipment used by the organizational units responsible for human resources.

4.3. Customers

The processing is carried out for the purpose of fulfilling contractual obligations towards customers, partners and suppliers of HOPS, for which there is a legal basis for processing. For processing legally based on the consent given by the subjects, the customers, partners and suppliers are informed via the consent form about the purposes of the processing and other relevant information that enable them to exercise their rights regarding personal data. All processing is done on the equipment located on the premises of HOPS.

4.4. Video surveillance

The video surveillance system is used to protect people and property. We keep the recordings obtained through the video surveillance system for a maximum of 15 days or longer if they are submitted as evidence in court, administrative, arbitration or other proceedings. At the request of competent authorities (police, court), video recordings can be submitted for carrying out procedures based on special regulations.

4.5. Recording telephone conversations in running the electric power system

In order for HOPS to ensure the continuous implementation of the legal obligation to operate the electric power system in accordance with the Transmission System Network Rules and the Operating Instructions Compilation, telephone conversations in running the electric power system and related tasks of HOPS are recorded in such a way that every conversation between the dispatchers of the National Dispatch Center, Network Centers and Remote Control Centres operators through end-user equipment, radio communication and telephone in running the electric power system and related tasks. Recordings of telephone conversations are automatically deleted by filling up the space on the hard disk of the digital voice recording system. At the request of competent authorities (police, court), recordings can be submitted for carrying out procedures pursuant to special regulations.

4.6. Processing personal data for marketing purposes

HOPS provides services on the basis of laws and regulations in the field of electric power transmission, as a rule, to legal entities. Due to the specific nature of its activity, HOPS does not, as a rule, have any natural person customers, nor does it process marketing information about them (e.g. profiling for the purpose of offering products and services, direct marketing, web marketing, etc.). When conducting marketing processing (e.g. communication with the public, special events, donations, sponsorships, etc.) requiring the consent of the subject, HOPS make it possible to give consent in accordance with the requirements of the GDPR Regulation.

4.7. Automated decision-making based on processing

At HOPS, we do not carry out processing on the basis of which automated decisions related to individuals are made.

4.8. Processing outside the territory of the Republic of Croatia

Occasionally, HOPS processes personal data outside the territory of the Republic of Croatia for the sake of international institutional cooperation and implementation of international projects. Such processing is carried out on the basis of bilateral or multilateral agreements with international organizations, financial institutions and partners that process personal data outside the territory of the Republic of Croatia, for the purpose of fulfilling the agreements in question. The method of collection and execution of processing and other details about the execution of such processing are defined through contractual clauses.

4.9. Privacy By Design rules

The application of appropriate measures to protect the personal data and privacy of respondents is mandatory in all new processing that we introduce into our business. For this purpose, when developing new products and services or any other type of processing, it is mandatory to follow the rules defined through the processes and procedures of design and development of new business processes, products and/or services. The managers of individual organizational units who make decisions on the purpose and means of processing personal data, the Data Protection Officer and the HOPS Management are responsible for regular monitoring and control of the application of these processes and procedures.

4.10. Assessment of the impact of personal data processing and risk assessment

HOPS is not obliged to assess the impact of personal data processing in accordance with the GDPR Regulation. HOPS will regularly analyze its operations, in order to identify in a timely manner the processing in which personal data is used, for which it is mandatory to carry out analysis and assessment of the impact of processing on personal data, including the risks arising from such processing, and will regularly carry this out. The assessment is carried out by the persons in charge of processing. For processing with medium and higher estimated effect, it is mandatory to carry out risk assessment and propose appropriate measures to mitigate the risk.

5. PERSONAL DATA STORAGE DURATION

We process personal data until the purpose of personal data processing is fulfilled. When the purpose for which they were collected has ended, we no longer use them, but they remain in our storage system and we keep them to the extent required by the legislation on maintaining archives.

6. PRINCIPLES OF PERSONAL DATA PROCESSING

HOPS processes personal data in accordance with the following processing principles:

- Legality, fairness and transparency of processing: personal data of all individuals (respondents) must be collected and processed legally, fairly and transparently. To this end, it is mandatory to inform each individual (respondent) in a clear and comprehensible manner about the purpose of collecting and processing personal data, the method and time of storage of such data, and the rights that respondents can exercise with regard to their personal data.
- Limitation of the purpose: the collection of personal data from the subject must be limited solely to fulfilling the obligations assumed by the contractual relationship with the subject or to fulfilling legal obligations

- Reduction of the amount of data: when collecting data from respondents, it is necessary to ensure the collection of only such personal data as are necessary to fulfill the purpose of individual processing
- Accuracy: in regular processing and control activities, it is mandatory to take appropriate measures to ensure the data are accurate and up-to-date and to make the necessary corrections or delete incorrect data without delay
- Limitation of storage: the preservation and storage of personal data in a form that enables the identification of the respondent is allowed only for as long as is necessary to fulfill the purpose of the processing, in accordance with defined internal and legal rules and data storage periods.
- Integrity and confidentiality: appropriate technical and organizational measures must be applied in all processing of personal data to ensure adequate security of personal data, which includes protection against unauthorized or illegal processing and protection against accidental loss, destruction or damage.
- Reliability: in the procedures for collecting and processing personal data, it is mandatory to provide appropriate records with which we can at any time prove the reliability and compliance of our processing with the above-mentioned principles.

7. EXCHANGE OF PERSONAL DATA WITH THIRD PARTIES

Personal data is transferred to third parties only in the following cases:

- For fulfilling the legal obligations of HOPS (obligatory data submitted to HZMO, HZZO, Tax Administration and other state institutions)
- For exercising the rights of workers under the Collective Agreement, the employment contract and other related regulations, the data is available to the processors by order and for the account of HOPS.

Processors process the data on the basis of a contract regulating the rules and obligations regarding the protection of personal data.

8. RIGHTS REGARDING THE PROCESSING OF PERSONAL DATA

8.1. The right to access personal data

The respondent has the right to access his/her personal data that we process and can request detailed information, in particular, about the purpose of the processing, about the type/categories of personal data that are processed, including insight into his/her personal data, about the recipients or categories of recipients, and about the expected duration of data storage. Access to personal data can only be limited in cases prescribed by EU legislation or

our national legislation, or when such a limitation respects the essence of the fundamental rights and freedoms of others.

8.2. The right to correct personal data

The respondent has the right to request correction or addition of personal data if such data is not accurate, complete and up-to-date. In order to do this, the respondent must send a request in writing to us as the controller, which also includes electronic communication. In the request, it is necessary to specify what is incorrect, incomplete or not up-to-date and how it should be corrected, and submit the necessary documentation in support the request.

8.3. Right to delete data

The respondent has the right to request that his/her personal data be deleted, if one of the following conditions is met:

- Personal data is no longer necessary to fulfil the purpose for which we collected or processed them
- The respondent withdraws his/her consent on which the processing is based (marketing and special categories of data) and there is no other legal basis for processing
- When the respondent lodges a complaint based on Art. 21 of the GDPR, and there is no stronger legitimate interest for processing
- Personal data is illegally processed
- Personal data must be deleted in order to comply with a legal obligation under EU law or the law of the country to which the controller is subject.

8.3.1. Exceptions related to the exercise of the aforementioned right are provided for in Article 17 paragraph 3 of the GDPR

The aforementioned rights shall not apply when processing is necessary:

- To exercise the right to freedom of expression and information;
- To comply with a legal obligation that requires processing under EU law or the law of a Member State to which the controller is subject, or to fulfil a task in the public interest or in the exercise of the controller's official authority;
- To maintain archives in the public interest, for scientific or historical research or for statistical purposes in accordance with Article 89 paragraph 1, when it is likely that the right from paragraph 1 may prevent or seriously jeopardize the achievement of the goals of that processing; or
- To establish, realize or defend legal claims.

8.4. The right to restrict the processing of personal data

The respondent has the right to obtain restriction of processing if:

- The respondent disputes their accuracy
- The processing is illegal and the respondent objects to the deletion of the data
- The data controller no longer needs the personal data, and the respondent requested it in order to establish, exercise or defend legal claims
- The respondent has objected to the processing of his personal data.

8.5. The right to object

If we process the respondent's data for the purposes of carrying out tasks in the public interest or in the exercise of our official powers, or in processing them we invoke our legitimate interests, the respondent can object to such processing.

9. USE OF INTERNET COOKIES (COOKIES)

On the official website www.hops.hr, we use the so-called cookies – text files placed on the user's computer by the web server, with the help of which the Internet Service Provider (ISP) displays the website. Cookies are created when the browser on the user's device loads the visited web destination, which then sends data to the browser and creates a text file (cookie). The browser retrieves and sends a cookie to the server of the website when the user returns to it.

10. PERSONAL DATA PROTECTION SYSTEM

We adhere to strict security procedures to reduce the risk of data destruction, unauthorized disclosure of data, unauthorized access to your data and other breaches. The equipment/premises on which we store personal data is located in a secure environment with limited physical access. We use firewalls, strong passwords, antivirus programs, and other measures to protect personal data. Only authorized persons at our facility have access to personal data, as regulated in our by-laws. We have obliged our workers to keep confidential all information they learn in the course of their work. We regularly organize training sessions for our employees so that the level of awareness of our society concerning personal data protection remains satisfactory.

11. SUPERVISORY BODY REPORTING AND ACTING ON BREACHES

Controllers establish and maintain the structure of responsibility for reporting incidents related to the security of personal data. In cases of breach of personal data, data controllers report to the supervisory authority without undue delay, possibly within 72 hours of becoming aware of it, unless it is unlikely that the breach of personal data will pose a risk to the rights and freedoms

of the individual. Any breach of security that leads to accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data that has been processed, stored or transmitted, is considered a breach of personal data.

12. AMENDMENTS TO PRIVACY POLICY

We regularly update our privacy policy so that it is always correct and up-to-date, and we reserve the right to make amendments to its content as we deem fit. You will be informed about all amendments in a timely manner through our website in accordance with the principle of transparency.

CHAIRMAN OF THE BOARD

DSc Igor Ivanković

July, 2023

CLASS: 700/23-15/90
NUMBER: 3-600-002/NS-23-03