KONČAR
D&ST

PERSONAL DATA PROTECTION POLICY

CONTENT

1 INTRODUCTION

This Personal Data Processing Policy applies to the processing of personal data carried out by KONČAR - DISTRIBUTIVNI I SPECIJALNI TRANSFORMATORI Inc. for production, Josipa Mokrovića 8, Zagreb, OIB 49214559889 (the **"Company"**) 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 or GDPR).

2 DATA CONTROLLER AND CONTACT DETAILS

The controller is KONČAR - DISTRIBUTIVNI I SPECIJALNI TRANSFORMATORI d.d. za proizvodnju, Josipa Mokrovića 8, Zagreb, OIB 49214559889.

To exercise your rights regarding the protection of personal data, you can contact us in the following ways:

- in writing to the following address: KONČAR - DISTRIBUTIVNI I SPECIJALNI TRANSFORMATORI d.d. za proizvodnju, Josipa Mokrovića 8, Zagreb, with the reference "Personal Data Protection"
- E-mail: personaldataprotection.dist@koncar.hr.

3 GENERAL PRINCIPLES OF PERSONAL DATA PROCESSING

Lawfulness, fairness and transparency - the processing of personal data must be based on a lawful legal basis (consent, legal obligation, legitimate interest, contract, public interest, vital interests of the data subject), and the information provided to the data subject must be concise, transparent, understandable and easily accessible.

Limited purpose - we collect and process personal data only for a specific and lawful purpose and do not further process them in a way that is inconsistent with the purpose for which they were collected.

Reducing the amount of data - we only use data that is appropriate and necessary to achieve a specific legitimate purpose.

Accuracy of personal data - in order to ensure fair and transparent data processing and to prevent possible misuse, personal data must be accurate, complete and up-to-date. It is extremely important for us that you notify us of any change and/or amendment to your personal data immediately or as soon as possible.

Restriction of data storage - personal data must be kept in a form that allows the identification of the data subject only for as long as necessary for the purposes for which the personal data is used.

Integrity and confidentiality - we process personal data in a secure manner, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage (e.g. access to personal data is granted only to authorized persons who need it to perform their work and have signed a confidentiality statement, and not other persons).

Principle of reliability - The controller is responsible for compliance with the Regulation and must be able to demonstrate it.

The Controller processes personal data only and to the extent that one of the following conditions is met:

a) the data subject has given consent to the processing of his/her personal data for one or more specific purposes

b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take actions at the request of the data subject prior to entering into a contract

c) the processing is necessary for compliance with the legal obligations of the controller

d) processing is necessary to protect the vital interests of the data subject or another natural person

e) processing is necessary for the performance of a task in the public interest or in the exercise of official authority of the controller

f) Processing is necessary for the purposes of the legitimate interests of the controller or a third party, except when these interests are overridden by the interests or fundamental rights and freedoms of the data subject that require the protection of personal data, in particular if the data subject is a child.

4 DATA SUBJECT RIGHTS

As part of the protection of personal data, data subjects have the following rights:

Right of access – the data subject has the right to obtain from the Controller a confirmation as to whether his/her personal data is being processed and, if such personal data are being processed, access to personal data and the purpose of processing, categories of data, potential recipients to whom the personal data will be disclosed, in accordance with the provisions of applicable law.

Right to rectification – the data subject has the right to obtain from the Controller the rectification of inaccurate personal data relating to him/her. Taking into account the purposes of the processing, the data subject has the right to complete incomplete personal data, including by providing an additional statement.

Right to erasure – the data subject has the right to obtain from the Controller the erasure of personal data relating to him/her, and the Controller is obliged to delete personal data without undue delay if one of the following conditions is met:

a) Personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,

b) The data subject withdraws the consent on which the processing is based, and there is no other legal basis for the processing,

c) The data subject objects to the processing, and no overriding legitimate grounds exist for the processing by the Controller which would outweigh the interests, rights or freedoms of the data subject,

d) Personal data has been unlawfully processed,

e) Personal data must be deleted in order to comply with a legal obligation.

Right to restriction of processing – The data subject has the right to request the restriction of processing if the following conditions are met:

a) The data subject disputes the accuracy of the personal data, for the period during which the controller is allowed to verify the accuracy of the personal data;

b) The processing is unlawful and opposes the erasure of the personal data and instead seeks the restriction of its use;

c) The controller no longer needs the personal data for the purposes of processing, but requires them for the establishment, exercise or defence of legal claims;

d) The data subject has filed an appropriate objection to the processing, awaiting confirmation as to whether the legitimate reasons of the Controller outweigh the reasons of the data subject.

Right to data portability - The Data Subject has the right to receive personal data concerning him/her, which he/she has provided to the Controller, in a structured, commonly used and machine-readable format and has the right to transmit this data to another controller without interference from the Controller, if the processing is based on consent or on a contract, or is carried out by automated means.

Right to object - The data subject has the right to object to the processing of personal data relating to him or her at any time.

Right to withdraw consent – The data subject has the right to withdraw his/her consent at any time, whereby the withdrawal of consent does not affect the lawfulness of processing based on consent before it was withdrawn.

Right to lodge a complaint with a supervisory authority – the data subject has the right to object to the processing of personal data to the Personal Data Protection Agency, azop@azop.hr.

The Company will take all measures to enable data subjects to exercise their rights if their exercise is possible within the framework of legal regulations.

5 TECHNICAL AND ORGANIZATIONAL MEASURES FOR THE PROTECTION OF PERSONAL DATA

The Controller implements appropriate technical and security protection measures aimed at ensuring the security and confidentiality of personal data processing, i.e. preventing unauthorized access or unauthorized disposal of personal data as well as technical equipment used by the Controller.

1. TECHNICAL MEASURES FOR THE PROTECTION OF PERSONAL DATA

Physical access control	Only authorized employees have access to the data processing systems. By the decision of the Management Board of the Company, persons authorized to process personal data have been appointed.
	Visitor Passes
	Enabling the locking of all premises related to data processing (includes access to premises and computer and other equipment used for data processing)
	Physical security of the premises where data transmitters are located
	Authentication at the entrance (port)
	Security alarm and other appropriate safety measures included outside of working hours
	Decentralization of data processing equipment and personal computers

	Physical protection measures (fencing, locked doors, front doors, windows)
	Restrictions on the availability of keys
	Identification of persons authorised to access
Data access and user control	Giving access only to individually determined individuals. By the decision of the Management Board of the Company, persons authorized to process personal data have been appointed.
	Rules for third parties (e.g. IT support).
	Terminal lock after a certain period of inactivity
	Protection of internal networks against unauthorized access (e.g. through firewalls)
	Implementation and maintenance of antivirus programs on all devices used for data processing
	Restricting access rights to only a limited number of administrators
	User passwords for data and programs
	Usernames and passwords (guidelines that include the length and time of their modification)
	Authentication of authorized persons
	Safeguards for data insertion, reading, blocking and deletion of stored data
	Automatic exclusion of the username after a password has been mistyped several times
	Using VPN technology
	Usernames and passwords on all devices
	Documenting access to applications (in particular insertion, modification, deletion and destruction of data)
	Using a log file for events (monitoring of system intrusion attempts)
	Guidelines for creating secure passwords provided to all employees
	Keeping records of data use
	Separation of production and test environments for databank and data
	Use of intrusion detection systems, anti-virus systems, firewalls for hardware and software (e.g. external data wiping)
	Deletion and destruction of all erasable data and electronic media (laptops, hard drives, USB sticks...) after the expiration of the contracted data processing
Transmission control	Use of document shredders or providers of such services
	Implementation of filtering measures (URL filter, filtering of e-mails, attachments, etc.)
	Storage / transfer of data in encrypted form

Check availability	Central procurement of hardware and software
	Rooms with servers are not located under the sanitary facilities
	Store backups outside of IT in a secure location
	Alternative Emergency Locations
	In flood hazard areas, server rooms are located above the water line
	Resilience of IT systems, even for cases of (very) high degree of use
	Fire protection measures (fire and smoke detectors, fire extinguisher in the server room)
	Create backups at regular intervals
	Verify that backups are established at regular intervals
	Placing the server in a separate secured room or data center
	A second server in a different location than the first one.
	Data mirroring
	Air conditioning in the room with the server
	Data Recovery Procedures
	Devices that monitor the temperature and voltage in server rooms
Data separation	Separation of productive and test systems
	Determination of rights to databases
Securing premises and physical documents	Paper documentation containing personal information must be kept in locked lockers and rooms

2. ORGANIZATIONAL MEASURES FOR THE PROTECTION OF PERSONAL DATA

Internal Policies and Policies	Personal Data Protection Rulebook; Personal Computer Equipment Rulebook; Rulebook on the Video Surveillance System, Personal Data Protection Policy; Information Security Rulebook; Organizational procedure – Timely notification of the management
Organizational and instructional control	Established authorizations for access to employees and third parties. By the decision of the Management Board of the Company, persons authorized to process personal data have been appointed.
	Guidelines for organizing data files
	Clean table policy
	Separation of functions between IT departments and other departments
	Existence of an emergency plan

	Appointment of the Security Officer
Confidentiality statement	All employees who process personal data for the controller sign a statement that they will process personal data in accordance with the legal provisions on the protection of personal data, as well as that they will implement appropriate protection measures over them and that they will not misuse them and give them to unauthorized third parties.
Personal Data Processing Agreement	A personal data processing agreement is concluded with each third party that processes personal data as a processor for the controller.
Employee education	Developing employee awareness of the importance of information security and data protection through periodic education.

6 ACCESS TO PERSONAL DATA

Access to the personal data of data subjects may be granted to employees of the Company who have limited rights of access and processing of data for the purpose of performing the tasks of their workplace and are obliged to maintain the confidentiality of personal data and act in accordance with the policies, procedures and other internal acts and contractually assumed obligations of the Company.
To the extent necessary and permitted by regulations, in order to achieve the purposes for which personal data were collected and/or processed, the Company may share them with third recipients such as:

- State and public authorities, judicial authorities or privately owned legal entities, when the Company is obliged to provide personal data on the basis of a legal obligation, or when it is necessary for the Company to protect its legitimate rights and interests,
- Service providers who provide certain services on the basis of special contracts, and may also act as processors,
- Business partners, to the extent that the transfer of personal data to such persons is necessary for the exercise of rights and obligations arising from or in connection with the employment relationship.
- Končar - Electrical Industry Inc. through the HRnet application for the purpose of consolidating the data of employees and candidates for employment by the Končar Group and adequate human resource management.

7 PROFILING

The Company does not carry out profiling.

8 EXPORT OF DATA TO THIRD COUNTRIES

The Company does not transfer personal data to countries outside the European Union and the European Economic Area.

9 PERSONAL DATA BREACH

In accordance with the provisions of the General Data Protection Regulation (GDPR), the Company has established a clear procedure for dealing with a personal data breach. In the event of a breach, the Company will take the following steps:

Notification to the competent authority

If a personal data breach may cause a risk to the rights and freedoms of individuals, the Company will report the breach to the competent authority for personal data protection (Personal Data Protection Agency – AZOP) no later than 72 hours from becoming aware of the breach. The report will list all relevant data, including the nature of the breach, the number of affected data subjects and records, the potential consequences, and the mitigation measures taken.

Informing data subjects

If the violation is likely to cause a high risk to the rights and freedoms of individuals, the Company will notify the affected data subjects without undue delay. The notification will contain information about the nature of the breach, the possible consequences, the measures taken to mitigate the damage, and contact details for further information.

Documenting the breach

The Company will keep a record of all personal data breaches, regardless of whether they are reported to the competent authority or not. The record will include the facts related to the breach, its consequences and the corrective actions taken.

Mitigation measures

The Company will immediately take appropriate technical and organizational measures to limit the consequences of the breach, such as identifying and eliminating the causes of the breach, preventing further data loss, and restoring system security.

10 RECORDS OF PROCESSING ACTIVITIES

The Company keeps records of processing activities for each type of personal data processing in accordance with applicable regulations in writing, including electronic form. The records shall include key information on the controller, the purpose of the processing, the legal basis, the categories of data and data subjects, the recipients, the security measures, the data retention period and, where applicable, the transfer of the data subject's personal data to third countries and the safeguards. This ensures transparency and compliance of all processing activities with the relevant legislation.

11 PROCESSORS

The Company engages processors for certain personal data processing activities, who process personal data on behalf of the Company and exclusively according to its instructions. Processors are selected on the basis of their expertise, reliability and ability to ensure appropriate technical and organizational data protection measures, in accordance with the provisions of the General Data Protection Regulation (GDPR).

All relationships with processors are regulated by a written contract that specifies the purpose of processing, duration, nature and type of personal data, obligations of the processor and data protection measures. The Company regularly monitors the work of processors to ensure their compliance with applicable regulations and data protection standards.

12 CHANGE OF POLICY

The Controller reserves the right to amend this Policy at any time, in accordance with applicable regulations and changes in internal personal data processing processes. All changes become effective on the day of publication of the updated version of the Policy.

The latest valid version of the Policy is always in force, and employees and other data subjects will be informed of its amendment in a timely manner in an appropriate manner.

13 ENTRY INTO FORCE

This Policy shall enter into force on the date of its adoption.

Zagreb, 22 July 2025

The Management Board of the Company:

Vanja Burul, President of the Management Board

NOTICE TO DATA SUBJECTS

ON THE PERSONAL DATA PROCESSING

22.07.2025.

CONTENT

1 INTRODUCTION

This Notice provides information on the purposes of processing, categories of personal data, retention periods, and other relevant aspects of the processing of personal data, carried out by KONČAR - DISTRIBUTIVNI I SPECIJALNI TRANSFORMATORI d.d. za proizvodnju, Josipa Mokrovića 8, Zagreb, OIB 49214559889 (the "Company")"), 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 or GDPR).

All details on the rights of data subjects, general principles of personal data processing and protective measures applied by the Company are prescribed in the Personal Data Protection Policy.

2 DATA CONTROLLER AND CONTACT DETAILS

The controller is KONČAR - DISTRIBUTIVNI I SPECIJALNI TRANSFORMATORI d.d. za proizvodnju, Josipa Mokrovića 8, Zagreb, OIB 49214559889.

To exercise your rights regarding the protection of personal data, you can contact us in the following ways:

- in writing to the following address: KONČAR - DISTRIBUTIVNI I SPECIJALNI TRANSFORMATORI d.d. za proizvodnju, Josipa Mokrovića 8, Zagreb, with the reference "Personal Data Protection"
- E-mail: personaldataprotection.dist@koncar.hr.

3 PROCESSING OF PERSONAL DATA THROUGH VIDEO SURVEILLANCE

The Controller uses the video surveillance system as a means of protecting persons and property - for safety at work, for the purpose of controlling entry to and exit from work areas and facilities, for reducing the exposure of workers and other persons to the risk of robbery, burglary, violence, theft and similar events at work or in connection with work, as well as for the purpose of protecting the property of the Controller, and for the purposes of disciplinary and criminal proceedings, if they are directly triggered by a security incident.

Video surveillance of the monitored area is carried out continuously, in a 24-hour period throughout the week.

The processing of personal data through video surveillance is regulated in detail by the Ordinance on the Video Surveillance System.

Purpose of processing	Technical protection of persons and property, control of entry and exit from work premises and premises.
Scope of processing	The video recording may contain personal data of persons (appearance of the person) and information about vehicles (registration number, vehicle description) moving at the location of the Company, as well as the date, time and location of the recording. The video surveillance system does not record audio.
Data subjects	Employees, business partners, visitors
Source	Data subject
Legal basis	Legitimate interest of the controller - Art. 6(1)(f) GDPR; An assessment of legitimate interests and an assessment of the impact of processing have been carried out.
Processor	The Company may use the services of a processor with whom it has concluded a personal data processing agreement.
Persons authorised to process	Employees according to the duties of the position, or according to the decision of the Management Board.
Data retention period	Surveillance camera recordings are kept for up to 40 days, after which they are automatically deleted. Recordings are reviewed only in the event of a security incident, in which case they are kept until the incident is resolved. In the event of a court dispute, the recordings may be used as evidence and retained until the final conclusion of the legal proceedings. The recording may be used for the purpose of conducting disciplinary proceedings against the Controller's employees in accordance with the Labour Act and the Controller's internal regulations.
Right of access	The right of access to the recordings is granted to persons authorized by the decision of the Management Board of the company, the Management Board of the company, as well as the competent state authorities based on special regulations.

4 PROCESSING OF PERSONAL DATA OF EMPLOYEES OF BUSINESS PARTNERS

The Company collects and processes personal data of employees of its business partners, where business partners are legal entities. The processing is limited exclusively to the contact details of employees that are necessary for the establishment and maintenance of business communication and the performance of contractual obligations between the Company and business partners.

Identification data	Name and surname
Contact data	Business Address, Business Phone Number, Business Mobile Phone Number, Business Fax Number and Business Email Address, Job Position
Other information	Further information necessarily processed in a project or contractual relationship with the Company, or voluntarily provided by a business partner
Purpose of processing	Execution of contracts and business cooperation with business partners, organization of business events
Source	Data subject
Legal basis	Compliance with the legal obligations of the controller - Art. 6(1)(c) GDPR; Execution of contracts to which the controller is a party - Art. 6(1)(b) GDPR; Pre-contractual actions - Art. 6(1)(b) GDPR; Legitimate interest of the controller - Art. 6(1)(f) GDPR
Persons authorised to process	Employees by job position
Retention period	Personal data is deleted when the retention of the personal data is no longer necessary in relation to the purpose for which it was processed, unless further retention is required by applicable legal, regulatory or accounting requirements. Business communications that are related to a contractual relationship are kept permanently for the purpose of protecting the legitimate interests of the controller. Since communication with business partners is related to the contractual relationship between the controller and business partners, the communication is kept permanently due to the need to prove the fulfilment of contractual obligations.

5 PROCESSING OF SHAREHOLDERS' PERSONAL DATA

The Company collects and processes the personal data of its shareholders for the purpose of fulfilling legal obligations, keeping records of shareholders and ensuring the exercise of rights related to the ownership of shares. The Company obtains information on shareholders from the Central Depository and Clearing Company (SKDD).

Identification data	Name and surname, OIB
Contact data	Address of residence/residence
Other information	Report on unpaid dividends (obtained from the SKDD)
Purpose of processing	Fulfilling legal obligations, keeping records of shareholders and ensuring the exercise of rights related to the ownership of shares
Source	Central Depository and Clearing Company (SKDD)
Legal basis	Compliance with the legal obligations of the controller - Art. 6(1)(c) GDPR Companies Act, Capital Market Law
Persons authorised to process	Financial Analyst
Recipients of personal data	SKDD, supervisory authorities based on a reasoned written request, shareholders based on the Companies Act
Retention period	The data is stored for 10 years.

6 PROCESSING OF PERSONAL DATA IN THE SELECTION PROCEDURE

The Company collects and processes personal data of candidates for employment for the purpose of conducting a selection procedure and assessing the suitability of candidates for open positions.

Identification data	Name and surname, OIB, date, place and country of birth, gender, citizenship, etc.
Contact data	Address of residence, e-mail address, telephone number
Information on education, qualifications and work experience	Personal education data, special knowledge, skills and abilities, other data specified in the candidate's CV, special exams and courses that are a requirement for performing the job (including licenses, certificates, etc.), driver's license number if it is a condition for performing the job, data on seniority and previous employment
Health data and special statuses	Data related to health if they are necessary for employment - certificate of medical fitness, status of a person with a disability, existence of an occupational disease, reduction of working capacity, risk of disability, data on established disability or physical impairment, etc.
Psychological testing results	The company may conduct psychological testing in the selection process to assess the qualities, abilities and skills of candidates applying for open positions. Psychological testing is based on the Society's legitimate interest in selecting the most suitable candidates for positions that require specific traits or skills. Candidates will be informed about the purpose and nature of the test, and their consent to participate in the test will be requested in advance.
Purpose of processing	Conducting the selection procedure and assessing the suitability of candidates for open positions
Source	Data subject
Legal basis	Until the end of the selection procedure, the consent of the respondent Art. 6(1)(a) GDPR; After the end of the selection procedure, the legitimate interest of the controller - Art. 6(1)(f) GDPR For storing of data in the candidates database for future job offers, the consent of the data subject Art. 6(1)(a) GDPR;
Persons authorised to process	Employees in the Department of Human Resources and General Affairs, organizational psychologist, external associates psychologists
Recipients of personal data	Supervisory authorities based on a reasoned written request, members of the selection committee
Data retention period	Personal data is retained for the duration of the selection procedure and deleted upon withdrawal of consent or after the procedure ends, whichever comes first. After the end of the competition, the data is kept for 6 months, after which it is automatically deleted. If the candidate gives consent to the further storage of data in the records for informing about future vacancies, the data is kept for this purpose until the consent is withdrawn, and no later than 12 months.

7 PROCESSING OF PERSONAL DATA OF THIRD PARTIES

The Company collects and processes the personal data of third parties, such as persons with whom a service contract has been concluded, pupils and students on practice and on the basis of a pupil or student contract, scholarship holders, for the purpose of fulfilling the obligations under the contract, monitoring and evaluating the performance and performing administrative and organizational tasks related to their engagement.

I. STUDENTS AND PUPILS

Identification data	Name and surname, OIB, gender, date of birth
Contact data	Address of residence, e-mail address, telephone number
Information on education, qualifications and work experience	Personal education data, special knowledge, skills and abilities, other data listed in the CV, special exams and courses that are a prerequisite for performing the job (including licenses, certificates, etc.), CV, working time records, contract
Financial data	Account number for the payment of the agreed fees
Psychological testing results	The Society may conduct psychological testing in the selection process for scholarship recipients in order to assess the qualities, abilities and skills of scholarship candidates. Psychological testing is based on the Society's legitimate interest in selecting the most suitable candidates for positions that require specific traits or skills. Candidates will be informed about the purpose and nature of the test, and their consent to participate in the test will be requested in advance.
Purpose of processing	Fulfilling contractual obligations from concluded contracts, conducting a selection procedure and assessing the suitability of candidates for open positions and scholarship holders.
Source	Data subject
Legal basis	Until the end of the competition, the consent of the respondent Art. 6(1)(a) GDPR; After the end of the tender, the legitimate interest of the controller - Art. 6(1)(f) GDPR For the storage of data in the database of candidates for future vacancies, the consent of the respondent Art. 6(1)(a) GDPR; After concluding the contract, compliance with the legal obligations of the controller - Art. 6(1)(c) GDPR; Ordinance on the Content and Manner of Keeping Records of Workers.
Persons authorised to process	Employees in the Human Resources and General Affairs Department, organizational psychologist, external associates psychologists, company secretaries
Recipients of personal data	Supervisory authorities based on a reasoned written request, members of the selection committee
Data retention period	Until the end of the competition, the data is kept until the withdrawal of consent. After the end of the competition, the data is kept for 5 years based on the legitimate interest of the controller. If the candidate gives consent to further storage of data in the records for informing about future vacancies, the data is kept until the consent is withdrawn, and no later than 2 years. After the conclusion of the contract, the data related to the calculation and payment of fees are kept for 11 years, and other data for 6 years from the termination of work with the controller, i.e. until the final termination of the dispute, if the controller has information that a labour dispute has been initiated regarding the exercise of rights arising from the employment relationship or in connection with the employment relationship.

II. EXTERNAL CONTRACTORS UNDER CONTRACTS FOR WORK

Identification data	Name and surname, OIB
Contact data	Address of residence, e-mail address, telephone number
Financial data	Account number for the payment of the agreed fees
Contract information	Concluded contract
Purpose of processing	Fulfilment of contractual obligations arising from concluded contracts
Source	Data subject
Legal basis	Compliance with the legal obligations of the controller - Art. 6(1)(c) GDPR
Persons authorised to process	Employees in the Human Resources Management, Legal and General Affairs Department
Recipients of personal data	Supervisory authorities based on a reasoned written request, employees regarding their job
Data retention period	After concluding the contract, the data related to the calculation and payment of fees are kept for 11 years in accordance with the Accounting Act. The contract for work is kept permanently.