PERSONAL DATA PROTECTION POLICY (INTERNAL for the organization not for data subjects)

(“Policy”)

|  |  |  |  |
| --- | --- | --- | --- |
| Title | Personal Data Protection Policy | | |
| Date | ${pzop\_01\_a} | Version | 1.0 |

**Controller:** ${pzop\_01\_b}

**Name and surname of authorized representative:** ${pzop\_01\_c}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of authorized representative

In line with the regulatory requirements of the 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 (hereinafter: **GDPR**) and the Act on the Implementation of the General Data Protection Regulation (hereinafter: **Law**), the controller ${pzop\_01\_d} (hereinafter: **the Controller**) adopts the following Personal Data Protection Policy (hereinafter: **Policy**).

1. Scope and objective

By adopting this Policy, the Controller aims to establish a data protection system in accordance with the GDPR. The policy establishes appropriate organizational measures to protect personal data of data subjects, i.e. clients, employees and business partners and other natural persons whose data are processed by the Controller.

2. Application

The Policy applies to all business processes involving in any way the processing of personal data carried out by automated and non-automated processing of personal data which forms part of the storage system, and obliges the Controller, all employees, as well as natural and legal persons working for and on behalf of the Controller.

3. Definitions

The terms used in this Policy have the same meaning as the terms used in the GDPR and the Law, and it is not necessary to mention them all, and as the basic terms of this Policy the following terms stand out:

**Personal data** – means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by means of identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to that individual’s physical, physiological, genetic, mental, economic, cultural or social identity

**Processing** – means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

**Controller** – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**Processor** - means any natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller;

**Personal data** **breach** – means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

4. Principles of data processing

The Policy is based on the following principles, in accordance with Art. 5 of the GDPR:

1. The principle of lawfulness, fairness and transparency – the processing of personal data must be based on one of the legal grounds (consent, legal obligation, legitimate interest, contract, public interest, vital interests of the data subject) and the information provided to data subject must be concise, transparent, understandable and easily accessible.
2. Purpose limitation principle – Personal data must be collected for specific, explicit and legitimate purposes and may not be further processed in a manner incompatible with those purposes.
3. The principle of data minimisation – personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. The principle of accuracy – personal data must be accurate, complete, up-to-date where necessary and corrected in a timely manner in the event of changes to the data. Every reasonable step must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. The principle of storage limitation – personal data must be kept in a form that allows the identification of the data subject only for as long as is necessary for the purposes for which the personal data are used.
6. Principle of integrity and confidentiality – data processing in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage through regular testing and the application of appropriate technical or organisational measures.
7. Accountability principle – the Controller is responsible for compliance with the GDPR and must be able to demonstrate it.

5. Processing of personal data

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

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes
2. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract
3. processing is necessary for compliance with a legal obligation of the Controller
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child

6. Purpose and scope of the processing of personal data

${pzop\_02}

${pzop\_02\_item}

${/pzop\_02}

7. Legal basis for the processing of personal data

${pzop\_03}

${pzop\_03\_item}

${/pzop\_03}

8. Retention period of personal data

The Controller shall ensure that data subjects are kept only for as long as is necessary to fulfil the purpose for which they were collected. Data for which there is no legal basis for further processing and storage shall be erased without delay.

${pzop\_04}

${pzop\_04\_item}

${/pzop\_04}

${pzop\_05}

9. Record of processing activities

The Controller shall keep a record of the processing activities for the personal data of the data subject which he or she regularly processes in the context of his/her business activities. Records shall be kept in writing, including in electronic form.

The records shall contain the following information:

* name and contact details of the Controller and the Data Protection Officer
* purpose of processing
* description of the category of data subjects and category of personal data
* category of recipients
* where applicable, transfer of personal data of the data subject to third countries and safeguards
* deadlines for deleting a category of data
* description of technical and organizational protection measures

${/pzop\_05}

10. Recipients of personal data

The Controller shall disclose the personal data of the data subject where the purpose of the processing so requires or where there is a legal obligation, in which case the personal data shall be disclosed to other natural or legal persons, public authorities, agencies or other bodies.

${pzop\_06}

11. Persons authorized to process personal data

Persons authorized to process personal data are determined by the responsible person within the Controller, and are determined with regard to the workplace and in accordance with the business processes they perform.

12. Technical and organizational measures

The Controller respects privacy and protects the personal data of its employees, business partners, clients, and whose personal data it processes in its day-to-day operations, in accordance with the provisions of applicable law.

The Controller shall ensure that the data subject’s data are kept only for as long as is necessary to fulfil the purpose for which they were collected.

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

Data storage is done using folders in the information system of the Controller and employees are granted access depending on the workplace.

Data storage is done using folders in the information system of the Controller and employees are granted access depending on the workplace.

13. Data protection impact assessment

Where a type of processing, in particular through new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

When carrying out a data protection impact assessment, the Controller shall seek advice from the Data Protection Officer.

A data protection impact assessment shall be required in particular in the case of:

1. systematic and extensive assessments of personal aspects relating to natural persons based on automated processing, including profiling, and on which decisions are made that produce legal effects relating to the natural person or similarly significantly affect the natural person;
2. processing on a large scale of special categories of personal data referred to in Art. 9(1) of the GDPR or data relating to criminal convictions and offences referred to in Art. 10 of the GDPR; or
3. systematic monitoring of a publicly accessible area to a large extent.

14. Notification of a personal data breach

In the event of a security incident, which complies with the GDPR, a personal data breach shall be carried out by the Controller without undue delay and shall, in accordance with the assessment, take the necessary action and inform the supervisory authority and the data subjects.

In the event of a personal data breach, the Controller shall notify the supervisory authority (the Personal Data Protection Agency) without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the reporting is not made within 72 hours, it shall be accompanied by the reasons for the delay.

The notification of a personal data breach shall include at least:

1. describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. provide the name and contact details of the data protection officer or other contact point from which further information can be obtained;
3. describe the likely consequences of the personal data breach
4. describe the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its potential adverse consequences.

If and to the extent that it is not possible to provide the above information at the same time, the information may be provided without undue delay.

The Controller shall document any personal data breaches, including facts relating to the personal data breach, its consequences and the measures taken to remedy the damage.

15. Processors

The Controller forwards personal data to its processors when it is necessary for the outsourcing of a particular business process. The employees of the Controller carry out an examination in the process of selecting the processor and verifying that the processors have adequate data protection controls, including appropriate technical and organisational measures for data protection.

The Controller enters into a data processing agreement with the processors requesting them to comply with the applicable policies of the Controller, the Law and the GDPR. Any data processing contract must contain the mandatory data referred to in Art. 28 of the GDPR. The Controller will allow the transfer of personal data to processors only if appropriate procedures are in place to ensure the required level of data protection.

16. Transfer of personal data to third countries

The Controller may transfer personal data to third countries only under the conditions and in the manner prescribed by the GDPR, subject to the conditions laid down in Chapter V of the GDPR, and the transfer is possible only on condition that the European Commission has taken a decision on an adequate level of protection with regard to a transfer to a given country which has been published in the Official Journal of the European Union or, in the absence of such a decision, provided that appropriate safeguards have been put in place by the Controller and provided that enforceable rights and effective judicial redress are available to data subjects, taking into account in particular the standard contractual clauses.

17. Data subjects’ rights

The Controller processes the personal data of the data subjects, in compliance with their rights as laid down in the GDPR.

Data subjects’ rights are as follows:

1. **The right to erasure (“right to be forgotten”)** – the data subject has the right to obtain from the Controller the erasure of personal data concerning him or her, and the Controller has the obligation to erase personal data without undue delay where one of the following grounds applies:

* personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
* the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;
* the data subject objects to the processing, and the legitimate grounds for exercising the right to erasure have greater weight than the legitimate interest of the Controller for the processing and/or storage of personal data,
* personal data have been unlawfully processed;
* personal data must be deleted in order to comply with a legal obligation;
* personal data have been collected in connection with the offer of information society services referred to in Art. 8(1) of the GDPR

1. **The right of access to data** – the data subject has the right to obtain from the Controller confirmation of whether his or her personal data are being processed and, where such personal data are processed, access to the personal data and the purpose of the processing, categories of data, potential recipients to whom the personal data will be disclosed, in accordance with the provisions of applicable law.
2. **The right to rectification** – the data subject has the right to obtain from the Controller the rectification of inaccurate personal data concerning him or her. Having regard to the purposes of the processing, the data subject shall have the right to complete incomplete personal data, including by making a supplementary statement.
3. **The right to object** – the data subject shall have the right, on grounds relating to his or her particular situation, to object at any time to processing of personal data concerning him or her in cases where processing is based on legitimate interest, including in cases of profiling. In cases where Controller processes personal data for the direct marketing purposes, the data subject has right to object to such processing at any time, and the Controller will stop processing of such data immediately and his/her personal data are no longer be used for this purposes.
4. **Right to restriction of processing** – the data subject has the right to request from the Controller the restriction of processing in the event that:
   * the accuracy of the personal data is contested by the data subject, for a period enabling the Controller to verify the accuracy of the personal data;
   * the processing is unlawful and the data subject opposes the erasure of personal data and requests the restriction of their use instead;
   * if the Controller no longer needs the personal data for the purposes of the processing, but the data subject requests them for the establishment, exercise or defense of legal claims, or
   * if the data subject has objected to the processing pending confirmation whether the legitimate reasons of the Controller outweigh the reasons of the data subject.
     1. **The right to data portability -** the datasubject shall have the right to receive the personal data concerning him or her which he or she has provided to a Controller in a structured, commonly used and machine-readable format and shall have the right to transmit those data to another controller without hindrance from the Controller to which the personal data have been provided, if the processing is based on consent, or on a contract or is carried out by automated means.
     2. **The right to object and automated individual decision-making** – the data subject has the right, on grounds relating to his or her particular situation, to object at any time to processing of personal data concerning him or her, including profiling based on those provisions. The Controller shall no longer process the personal data unless the Controller can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defense of legal claims. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for the purposes of such marketing, including profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. At the latest at the time of the first communication with the data subject, the above rights must be explicitly brought to the attention of the data subject and must be done in a clear and separate manner from any other information.
     3. **The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling**, which produces legal effects concerning him or her or similarly significantly affects him or her. This shall not apply if the decision:

|  |  |
| --- | --- |
|  | * necessary for the conclusion or performance of a contract between the data subject and the data Controller; |

|  |  |
| --- | --- |
|  | * authorised by Union or Member State law to which the Controller is subject, and which also provides for suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or |

|  |  |
| --- | --- |
|  | * based on the data subject’s explicit consent. |

* + 1. In addition, the data subject has the **right to lodge a complaint with the competent supervisory authority** (in the Republic of Croatia – the Personal Data Protection Agency) and to be informed about the recipients or categories of recipients to whom the data have been or will be disclosed in the future, and in particular recipients in third countries.

18. Exercise of the rights of the data subject

${pzop\_13}

The Controller to the data subject upon request to exercise the rights referred to in point 13 of the Policy, provide the information without undue delay and in any event within one month of the date of receipt of the request;

If the Controller does not act on the request of the data subject, the Controller shall inform the data subject without delay and no later than one month of receipt of the request of the reasons for not acting and of the possibility of lodging a complaint with the supervisory authority (Personal Data Protection Agency).

19. Data Protection Officer

In order to coordinate and supervise the operations of the Controller in accordance with the provisions of the GDPR, the Controller has appointed a Data Protection Officer. Data on the Data Protection Officer are reported to the Agency for Personal Data Protection and the Data Protection Officer communicates with the Agency in case of questions or supervision.

The Data Protection Officer serves as a contact point for all data subjects and responds to the data subject’s requests in accordance with the GDPR and the procedures of the Controller.

All employees are obliged to notify the Data Protection Officer of any personal data breach and the officer will participate in the risk assessment of the breach and give his/her opinion on the risk and measures.

Employees contact the Data Protection Officer in case of new business cooperation, doubts about the processing of personal data whereby the officer performs appropriate analyses of legitimate interest and data protection impact assessments, in accordance with the decision of the Agency and the GDPR, verification of technical and organizational measures of the processor, supervision of processors and consultation in the composition of business cooperation contracts and data processing contracts.

The Data Protection Officer also checks transfers of personal data to third countries and proposes appropriate safeguards for the transfer of data (e.g. standard contractual clauses).

The Data Protection Officer is obliged to draw up a training plan for employees of the Controller every year and to conduct or arrange regular training of relevant employees at least once a year on the topic of data protection.

The Controller shall provide adequate resources and training to the data protection officer for the performance of his or her tasks in accordance with the GDPR.

The Data Protection Officer is obliged to monitor the compliance of the Controller’s business with this Policy and at least once a year submit to the Management Board of the Controller a report on the status of the Controller’s compliance with the GDPR and the measures taken.

20. Final provisions

The Policy enters into force eight days from the date of signature and is published on the notice board/internal network of the Controller.