**INDUSTROOPREMA d.o.o.**
Zagreb, Obrtnička 1

# PRIVACY POLICY

## 1. INTRODUCTORY PROVISIONS

This Policy is adopted with due regard to and 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; Official Journal of the European Union L 119 of 4 May 2016), as implemented pursuant to the Act on the Implementation of the General Data Protection Regulation (Official Gazette No. 42/18).

This Policy sets out the fundamental rights and obligations of the controller and data subjects, establishes rules of conduct for the controller's employees, and defines the expected conduct of the controller's business partners who process personal data on behalf of the controller or who come, or may come, into contact with such data.

This Policy also establishes measures that give particular effect to the principles of data protection by design and by default, for the purpose of protecting the rights and freedoms of individuals with regard to the processing of personal data.

## 2. DEFINITIONS

**PERSONAL DATA**
Any information relating to an identified or identifiable natural person (data subject).

**PROCESSING**
Any operation or set of operations 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**
INDUSTROOPREMA d.o.o. (the entity that determines the purposes, means and manner of processing).

**PROCESSOR**
A natural or legal person or another body that processes personal data on behalf of the controller.

**DATA SUBJECT**
A natural person - the individual whose personal data are processed.

**PERSONAL DATA BREACH**
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

*For more detailed definitions, reference is made to Article 4 of the General Data Protection Regulation.*

## 2. PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

The principles relating to the processing of personal data are as follows:

**LAWFULNESS, FAIRNESS AND TRANSPARENCY**
Personal data shall be processed lawfully, fairly and transparently in relation to the data subject.

Processing is lawful where it is based on at least one of the legal grounds laid down in the General Data Protection Regulation. The controller shall process personal data where:

- the data subject has given consent to the processing for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 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;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring the protection of personal data, in particular where the data subject is a child.

Processing is fair and transparent where the data subject has been informed of the processing and its purposes and the processing is carried out accordingly.

Transparency means that it must be clear to the individual/data subject how personal data relating to them are collected, used, disclosed or otherwise processed, and the extent to which those data are or will be processed.

**PURPOSE LIMITATION**

Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes.

**DATA MINIMISATION**

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

**ACCURACY**

Personal data shall be accurate and, where necessary, kept up to date. The controller shall take every reasonable step to ensure that personal data that are inaccurate are erased or rectified without delay.

**STORAGE LIMITATION**

Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

**INTEGRITY AND CONFIDENTIALITY**

Personal data shall be processed and stored in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical or organisational measures.

## 3. RIGHTS OF DATA SUBJECTS

Where the controller collects personal data relating to a data subject directly from that data subject, the controller shall provide the information referred to in Article 13 of the General Data Protection Regulation at the time the data are obtained.

Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the information referred to in Article 14 of the General Data Protection Regulation.

Where the controller intends to further process personal data for a purpose other than that for which the data were collected, the controller shall, prior to such further processing, provide the data subject with information on that other purpose and with all other relevant information required by the General Data Protection Regulation (Article 13(3) / Article 14(4)).

The foregoing obligations to provide information do not apply if and to the extent that the data subject already has the information.

All data subjects whose personal data are collected and processed by the controller have the following rights:

**RIGHT OF ACCESS**

The data subject has the right to obtain confirmation as to whether personal data concerning them are being processed and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient;
- where possible, the envisaged period for which the personal data will be stored or, if this is not possible, the criteria used to determine that period;
- the existence of the right to request rectification or erasure of personal data, restriction of processing, or to object to such processing;
- the right to lodge a complaint with the competent supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making and, in the cases and under the conditions prescribed by law, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Where personal data are transferred to a third country or an international organisation, the data subject has the right to be informed of the appropriate safeguards relating to the transfer.

The controller shall provide a copy of the personal data undergoing processing; however, that right shall not adversely affect the rights and freedoms of others.

**RIGHT TO RECTIFICATION**

The data subject has the right to obtain the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject also has the right to have incomplete personal data completed.

**RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)**

The data subject has the right to obtain the erasure of personal data where one of the conditions laid down in the Regulation is met.

**RIGHT TO RESTRICTION OF PROCESSING**

The data subject has the right to obtain restriction of processing where one of the conditions laid down in the Regulation is met.

**RIGHT TO DATA PORTABILITY**

The data subject has the right to receive personal data concerning them and to transmit those data to another controller where one of the conditions laid down in the Regulation is met.

**RIGHT TO OBJECT**

The data subject has the right, on grounds relating to their particular situation, to object at any time to the processing of personal data.

**RIGHT REGARDING PROFILING AND AUTOMATED DECISION-MAKING**

The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

**OTHER RIGHTS AND LIMITATIONS**

The data subject also enjoys any other rights provided for by the General Data Protection Regulation and/or the Act on the Implementation of the General Data Protection Regulation, even if such rights are not expressly set out in this Policy. The rights referred to above do not exclude any restrictions on their exercise prescribed by the Regulation or other applicable laws, and the provisions of this Policy do not grant the data subject rights beyond those prescribed by the Regulation. The Regulation and other applicable laws shall therefore apply in full in each individual case.

## 4. SECURITY AND PROTECTION OF PERSONAL DATA

The controller shall implement, and the processor shall also be required to implement, appropriate technical and organisational measures to ensure a level of security appropriate to the risk of a personal data breach, including, where appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

The controller shall take, and the processor shall be required to take, measures to ensure that any natural person acting under the authority of the controller or processor who has access to personal data processes those data only on instructions from the controller, unless required to do so by European Union law or the applicable laws of the Republic of Croatia.

Technical and organisational measures are implemented to protect personal data and prevent personal data breaches. Such measures reduce the risk of a personal data breach.

When determining appropriate measures, the controller shall assess the appropriate level of security, taking particular account of the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Technical safeguards:**

- Personal data, irrespective of the form or medium in which they are collected (personnel files, files containing personal data, binders, CDs and similar media), shall primarily be kept under lock and key. This means that they shall be stored in locked cabinets, drawers or rooms. Personal data may also be stored in another appropriate manner, but must at all times remain under the supervision of an authorised person and be inaccessible to unauthorised persons.
- All computers and devices of the controller (PCs, laptops, tablets, etc.), as well as devices connected to the controller's network, must have appropriate antivirus protection.
- Access to all computers and devices of the controller must be password-protected. Passwords must not be disclosed to other persons.
- The controller shall ensure appropriate data backups.
- All computers, devices and other IT equipment of the controller may be used exclusively for the performance of business duties.
- Electronic mail shall be used exclusively for business purposes.
- Any loss, theft, damage or unauthorised use of equipment or materials containing personal data, of personal data themselves, or of a personal data filing system must be reported immediately to the controller's responsible person.
- Any detected presence of a computer virus must be reported immediately to the controller's responsible person.
- Audio or video recording and photography on the controller's premises or during activities related to the controller's business are prohibited unless approved by the controller.

- IT equipment disposed of as waste shall be handled appropriately; before it is handed over for disposal, all data stored on the equipment must be permanently destroyed or erased.

**Organisational safeguards:**

- Personal data shall be collected and processed by persons specifically authorised by a decision of the controller, or by persons whose job duties and position inherently require such processing, in all cases in accordance with the controller's instructions. The same applies to processors.
- The controller shall organise work processes so that personal data are not accessible to unauthorised persons and so that authorised persons have access only to the extent strictly necessary.
- The controller shall require its employees to sign confidentiality statements or shall ensure the obligation to protect personal data through appropriate provisions in employment contracts, annexes to employment contracts or separate agreements. The same shall be required of persons performing work for the controller under service contracts or similar agreements.
- Employees of the controller and persons performing work under service contracts or similar agreements shall maintain the confidentiality of all personal data contained in the controller's records to which they have access, as well as all other personal data relating to employees, business partners or any third parties of which they become aware in the course of their work, even accidentally. This duty applies both to data they are authorised to access and to any other data of which they become aware, and continues after their authority to access personal data has ceased.
- The controller shall enter into an appropriate agreement with each processor for the purpose of ensuring the protection of personal data.
- The controller shall require every individual or third party, irrespective of their status in relation to the controller, who acts under the authority of the controller or processor and may gain access to personal data through the business relationship, to protect such data. As a rule, this obligation shall be established in writing by means of a statement, agreement or contractual clause.
- The controller shall issue instructions on the handling and protection of personal data and, where necessary, provide appropriate training to employees and third parties.

The controller may also determine and establish safeguards by separate decisions or implement them through the organisation of its business operations.

## 5. RECORDS, BREACH REPORTING AND BREACH NOTIFICATION

The controller shall maintain all records required under the General Data Protection Regulation and shall retain personal data for the shortest period necessary, adopting separate decisions for individual cases where appropriate.

In the event of a personal data breach, the controller shall, without undue delay and, where feasible, not later than 72 hours after becoming aware of it, notify the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where notification is not made within 72 hours, it shall be accompanied by reasons for the delay (Article 33 of the General Data Protection Regulation).

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay (Article 34 of the General Data Protection Regulation).

## 6. FINAL PROVISIONS

In addition to this Policy, the controller may adopt other policies relating to specific areas of personal data processing. In such cases, those policies shall form an integral part of the controller's personal data protection policies.

This Policy shall in no way diminish, restrict, amend or repeal the provisions, rights and obligations prescribed and established by the General Data Protection Regulation and other applicable laws. Any matter not expressly regulated by this Policy but governed by the General Data Protection Regulation and/or other applicable laws shall apply in full. For more detailed rules concerning rights and obligations relating to the protection of personal data, this Policy refers to the General Data Protection Regulation and the Act on the Implementation of the General Data Protection Regulation.

The controller shall familiarise all its employees and all persons who process personal data with this Policy.

This Policy enters into force on the date of its adoption.

Zagreb, 25 May 2018

**Director:**