

Privacy and personal data protection policy - GDPR act

In Zagreb, July 1, 2024

CONTENT

1	INTRODUCTION	2
2	PRIVACY AND PERSONAL DATA PROTECTION POLICY	3
2.1	GENERAL REGULATION ON DATA PROTECTION	3
2.2	DEFINITIONS	3
2.3	PRINCIPLES OF PERSONAL DATA PROCESSING	4
2.4	RIGHTS OF INDIVIDUALS	5
2.5	LEGALITY OF DATA PROCESSING	6
2.5.1	CONSENT	6
2.5.2	EXECUTION OF THE CONTRACT	7
2.5.3	COMPLIANCE WITH LEGAL OBLIGATIONS	7
2.5.4	KEY INTERESTS OF RESPONDENTS	7
2.5.5	PROCESSING IS NECESSARY FOR PERFORMING A PUBLIC INTEREST TASK	7
2.5.6	LEGITIMATE INTERESTS	8
2.6	TECHNICAL PROTECTION OF PRIVACY	8
2.7	AGREEMENTS INVOLVING THE PROCESSING OF PERSONAL DATA	8
2.8	CROSS-BORDER TRANSFER OF PERSONAL DATA	8
2.9	PERSONAL DATA PROTECTION OFFICER (DPO)	9
2.10	RECORDS OF PROCESSING ACTIVITIES	9
2.11	NOTICE OF BREACH OF PERSONAL DATA (DATA BREACH) AND THE RIGHT TO COMPLAINT	9
2.12	COMPLIANCE WITH GENERAL REGULATION	10
2.13	FINAL PROVISIONS	11

List of tables

<i>TABLE 1 - DEADLINES FOR RESPECTING THE RIGHTS OF RESPONDENTS</i>	<i>6</i>
---	----------

1 Introduction

In its daily business, **LOKL Dizajn Market doo** Zagreb, Siget 20B, OIB: 85212629376 (hereinafter: the Company) uses various personal data of persons, on the basis of which their identity can be determined, including data on:

- current, former and future employees
- customers, suppliers, business partners
- to the owner/owners
- guests at events organized by the Company
- to persons entering the Company's business premises
- to visitors of the company's website <https://lokl.hr/>
- colleagues

In collecting and using the aforementioned data, the Company acts in accordance with the relevant regulations that determine the manner in which such activities are carried out and that determine the protective measures that must be provided in order to protect such activities.

The purpose of this policy is to determine the applicable regulations and describe the steps the Company takes to ensure that such behavior is in accordance with the applicable regulations.

This control applies to all systems, persons and processes that form an integral part of the organization's information system, including board members, employees, suppliers and other third parties who have access to the Company's information system.

Purpose of the document

The personal data protection policy (hereinafter: the Policy) is a fundamental act that describes the purpose and goals of the collection, processing and management of personal data by the company **LOKL Dizajn Market doo** Zagreb, Siget 20B, OIB: 85212629376 (hereinafter: Company).

The goal of the Policy is to establish appropriate processes for the protection and management of personal data of respondents, service users, customers, partners, employees and other persons whose personal data is processed, in accordance with the provisions of the General Data Protection Regulation 2016/679 (hereinafter: Regulation), legal regulations and internal acts of the Company.

2 Privacy and personal data protection policy

2.1 General Data Protection Regulation

The General Data Protection Regulation 2016 (hereinafter: General Regulation) is one of the most important regulations that determines how the Company performs its activities related to the processing of personal data. High fines are prescribed in cases of actions contrary to the General Regulation, which were determined in order to protect the personal data of citizens of the European Union. The company's policy ensures compliance with the General Regulation and other relevant regulations in a clear manner that can be proven at any time.

2.2 Definitions

The general regulation lists 26 definitions, and it is not necessary to list all definitions in this document. However, the following definitions stand out as the basic definitions of this Policy:

"Personal data" means:

any data relating to an individual whose identity has been determined or can be determined ("the respondent"). Respondent - a person/individual whose identity can be determined directly or indirectly, especially with the help of identifiers such as name, identification number (OIB, JMBG, etc.), location data, network identifier or with the help of one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

"Processing of personal data" means:

any procedure or set of procedures performed on personal data or sets of personal data, whether by automated or non-automated means such as collection, recording, organization, structuring, storage, adaptation or modification, retrieval, inspection, use, disclosure by transmission, dissemination or otherwise making available, matching or combining, restricting, erasing or destroying.

"Controller" means:

natural or legal person, public authority, agency or other body that alone or together with others determines the purposes and means of personal data processing; when the purposes and means of such processing are determined by the law of the Union or the law of a Member State, the controller or special criteria for his appointment may be provided for by the law of the Union or the law of a Member State.

"Processor" means:

*natural or legal person, state administration bodies and other state bodies, local and regional units
(regional) self-government, agency or other body that processes personal data on behalf of the controller.*

"Information system" means:

a combination of technological infrastructure, organization, people and procedures for collecting, processing, storing, transmitting, generating, displaying and distributing information as well as disposing of it. It is possible

also defined as the interaction of information technology, data and data processing procedures and the people who collect and use said data.

"Supervisory body" means:

The Agency for the Protection of Personal Data, that is, an independent body of public authority established by the Republic of Croatia for the purpose of controlling and ensuring the implementation of the Regulation (hereinafter: AZOP).

"Consent" means:

any voluntary, special, informed and unequivocal expression of the wishes of the subject by which he gives his consent to the processing of personal data relating to him by a statement or a clear affirmative action

2.3 Principles of personal data processing

These are the basic rules that the Company adheres to when processing personal data of respondents.

Legal processing is those that are carried out in accordance with the described principles. Every employee of the Company who processes personal data is obliged to adhere to the described principles when processing personal data of respondents.

There are several basic principles on which the General Regulation is based.

These principles are as follows:

1. Personal data must be:

- (a) lawfully, fairly and transparently processed with respect to the data subject ("lawfulness, fairness and transparency");*
- (b) collected for specific, explicit and lawful purposes and may not be further processed in a manner inconsistent with those purposes;*
- (c) appropriate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data reduction");*
- (d) accurate and as necessary up-to-date; every reasonable measure must be taken to ensure that personal data that is inaccurate, taking into account the purposes for which it is processed, is deleted or corrected without delay ("accuracy");*
- (e) stored in a form that allows identification of the data subject only for as long as it is necessary for the purposes for which personal data is processed; Personal data of respondents can be stored even longer for reasons prescribed by law (e.g. the Act on Archive Material and archives) or due to the Company's legitimate interest (e.g. prescribed claims limitation periods*

by the Law on Obligatory Relations, Court Disputes) ("storage limitation").

(f) processed in a way that ensures adequate security of personal data, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage by applying appropriate technical or organizational measures ("integrity and confidentiality");

(Mr) processing of personal data based on the consent given by the respondent for one or more purposes

*(The company must be able to prove that the respondent gave it). Request for written consent of the respondent must be presented in such a way that it can be clearly distinguished from other questions, u
in an understandable and easily accessible form with the use of clear and simple language.*

2. The controller is responsible for compliance with paragraph 1 and must be able to prove it ("reliability").

The company ensures compliance with the stated principles both in the processing of personal data that is currently carried out, as well as in the introduction of new methods of processing personal data, such as new IT systems.

2.4 Rights of individuals (respondents)

The respondent has certain rights in accordance with the General Regulation . The rights of respondents consist of the following rights:

1. the right to information

When collecting personal data, the respondent is also provided with information about identity and contact information

of the controller/Company, contact details of the data protection officer, legal basis for processing and purpose of processing for which his personal data are used, whether the processing is based on the legitimate interest of the Company or a third party, recipients or categories of recipients of his data, intention to transfer data to of third countries (if there is an intention), the criteria by which the period of storage of such data was determined, about his other rights (access to data, deletion or correction of data, the right to object, to limit processing and to data portability), about the right to object AZOP- in, on the right to withdraw consent (where it was necessary).

2. the right to access data

The respondent has the right to receive confirmation as to whether his personal data is being processed and, if processed, access to that data

3. right to data correction

The respondent has the right, without undue delay, to obtain from the data controller the correction of inaccurate personal data relating to him.

4. right to delete data (right to be forgotten)

The respondent has the right to obtain the deletion of personal data relating to him, and the Company has the obligation to delete personal data without undue delay if one of the following conditions is met: personal data

are no longer necessary for the purposes for which they were collected, the respondent withdraws his consent to the processing based, the respondent lodges an objection to the processing of personal data, personal data have been illegally processed and personal data must be deleted in order to comply with legal obligations.

5. the right to restrict data processing

The respondent has the right to obtain a limitation of data processing if one of the following conditions is met: the respondent disputes the accuracy of the personal data, the processing is illegal and the respondent opposes erasure and instead requests a restriction of data use, the Company no longer needs personal data for processing purposes, the respondent has invested objection based on legitimate interest.

6. the right to data portability

At the request of the data subject, the Company can provide him with personal data in a structured, commonly used and machine-readable format, and the data subject has the right to transfer them to another data controller, provided that data processing is based on consent or if it is necessary for the execution of a contract to which the data subject is a party or in order to take actions at the request of the respondent before concluding the contract, and if the processing is carried out by automated means.

7. the right to file a complaint

The data subject has the right, based on his particular situation, at any time to object to the processing of data when it is processed on the basis of the legitimate interest of the Company or a third party, including the creation of a profile based on these grounds. In this case, the Company may no longer process personal data unless it proves that there are compelling legitimate reasons for processing that go beyond the interests, rights and freedoms of the data subject or for the purpose of exercising or defending legal claims. The respondent has the right at any time to object to the processing of personal data for the purpose of direct marketing, which includes creating a profile to the extent related to such direct marketing, in which case the Company may no longer process the data for these purposes.

8. rights related to automated decision-making and profiling

The respondent has the right not to be subject to a decision based solely on automated processing, including the creation of a profile, when these decisions produce legal effects in relation to him or similarly significantly affect him, except in the case when such a decision is necessary for concluding and executing a contract between the respondent and the Company, when it is permitted by some other legal regulation or when it is based on the express consent of the respondent

Each of the above-mentioned rights are guaranteed, and the deadlines shown in table 1 are provided for respecting the above-mentioned rights of the respondents, all in accordance with the General Regulation.

Respondent's request	Deadline
Right to information	During data collection (if data is collected from respondents) or within one month (if data is collected from another source)
Right to access data	One month from the receipt of the request
Right to rectification of data	One month from the receipt of the request
The right to delete data	Without unnecessary delay
The right to restrict data processing	Without unnecessary delay
The right to data portability	One month from the receipt of the request
The right to submit a complaint	At the time of receiving the complaint
Right in relation to automated decision-making and profiling	Not determined

2.5 Legality of data processing

There are six alternative ways to achieve the legality of personal data processing in each individual case, in accordance with the General Regulation . It is the task of the Company to identify and document the basis for the processing of basic data in accordance with the General Regulation .

The options are briefly described in the sections below.

2.5.1 Constraint

The company always obtains the express consent of the respondent for the collection and processing of his personal data, except in cases where it is not required for reasons permitted by the General Regulation . In the case when the respondent is a child under the age limit of 16 years (some states

member states may provide for a lower age limit), it is necessary to obtain the consent of the child's parents.

We will provide respondents with transparent information about the use of their personal data at the time they give their consent, and we will also explain their rights in relation to personal data, such as the right to withdraw consent.

The above information will be provided free of charge and in an accessible form, written in clear language.

If personal information is not collected directly from the data subject, the same information will be provided to the data subject

- a) within a reasonable time after the data has been collected and no later than within one month, or
- b) if the data is used for communication with the respondent, at the latest at the moment of the first communication with that respondent; or
- c) if disclosure of data to another recipient is foreseen, at the latest at the time when personal data was first disclosed.

2.5.2 Contract execution

The express consent of the respondent is not required if the collection and processing of personal data is necessary for the fulfillment of a contract to which the respondent is a party. This will often be the case when the contract cannot be executed without the collection and processing of personal data, for example, the delivery cannot be executed without the delivery address.

2.5.3 Compliance with legal obligations

Explicit consent of the subject is not required if personal data is collected and processed in order to comply with legal obligations. This can be in the case of certain data related to employment and taxation, as well as in cases related to the field of activity of the public sector.

2.5.4 Key interests of respondents

In the event that personal data is necessary to protect the key interests of the data subject or another natural person, then the same constitutes a legal basis for the processing of personal data. In cases where the stated reason is used as a legal basis for collecting personal data, the Company will act reasonably when assessing the existence of a legal basis and document evidence that confirms the existence of such a legal basis for collecting personal data. For example, the stated basis can be used in aspects of social welfare, especially in the public sector.

2.5.5 Processing is necessary for the performance of a task of public interest

If the Company needs to perform a task that it believes is in the public interest or that is necessary for the performance of an official duty, then the express consent of the respondent is not required. The assessment of public interest or official duty shall be documented and made available as evidence in case of need.

2.5.6 Legitimate interests

If the processing of specific data is necessary to protect the legitimate interests of the Company and if it is considered that it does not significantly affect the rights and freedoms of the data subject, then it may represent a legitimate reason for processing personal data. The justification for the existence of the stated reason must be documented.

2.6 Technical privacy protection

The company has adopted the principle of technical privacy protection and will ensure that the definition and planning of all new or significant changes to systems that collect or process personal data are subject to privacy protection rules, including the implementation of one or more personal data protection impact assessments.

Assessment of the impact of personal data protection includes:

- consideration of how personal data will be processed and for what purposes
- assessment of whether the proposed processing of personal data is necessary and proportionate to the purpose/purposes
- risk assessment for individuals in the processing of personal data
- which controls are necessary to address identified risks and to demonstrate compliance with regulations.

The use of techniques such as the reduction of personal data and pseudonymisation will be considered where applicable and appropriate.

2.7 Contracts involving the processing of personal data

The Company will ensure that all relationships it enters into, which include the processing of personal data, will be the subject of a written contract, which includes specific information and conditions prescribed in the General Regulation.

2.8 Cross-border transfer of personal data

The transfer of personal data outside the European Union or the European Economic Area is carefully checked before the transfer itself to ensure compliance with the framework imposed by the General Regulation. The aforementioned transfer depends in part on the judgment of the European Commission regarding the suitability of the personal data protection measures applied in the receiving country, and this may change over time.

The international transfer of personal data within the group is subject to legally binding agreements that represent the binding corporate rules of Art. 47. General regulations guaranteeing the rights of data subjects, in the absence of which the Company will use standard contractual clauses on data protection.

2.9 Personal Data Protection Officer (DPO)

The role of the Personal Data Protection Officer (DPO) is defined and binding in accordance with the General Regulation if the organization is a public authority, if it carries out large-scale monitoring of personal data or if it processes particularly sensitive types of personal data on a large scale. The personal data protection officer must have an appropriate level of knowledge, and may be a staff member or perform tasks based on a work contract.

Based on the above criteria, the Company is obliged to appoint a Personal Data Protection Officer, and in that case it will inform the supervisory authority about his data.

2.10 Records of processing activities

The company is obliged to keep records of processing activities, and the records must contain:

- *the name and contact details of the controller and, if applicable, the joint controller and personal data protection officer*
- *processing purposes*
- *description of categories of respondents and categories of personal data*
- *categories of recipients to whom personal data has been disclosed or will be disclosed, including recipients in third countries or international organizations*
- *if applicable, transfers of personal data to a third country or international organization, including identification of that third country or international*

*organization, and in accordance with the conditions prescribed by the Regulation,
documentation on appropriate protective measures*

- *provided deadlines for the deletion of different categories of data, if possible and*
- *a general description of technical and organizational security measures, if possible*

2.11 Notification of a personal data breach (DATA BREACH) and the right to file a complaint

The Company's policy must be fair and proportionate when considering the actions that need to be taken in order to inform the respondents on whose side the personal data breach occurred.

In accordance with the General Regulation, all employees of the Company have the duty to inform the personal data protection officer in the event of an incident related to the protection of personal data, and in the event of a violation, the Company is obliged to notify AZOP within 72 hours, after learning about the violation, if it is feasible.

If the respondent has any questions about how the Company uses his personal data or wishes to file an objection to the processing of personal data, he can contact the personal data protection officer directly at e-mail _____.

By indisputably establishing the identity of the respondent (by copying a document with the respondent's handwritten signature if the request is sent via email), the Company will act on the respondent's submitted request.

If the Company has justified doubts regarding the determination of your identity when submitting a request, the Company may, in accordance with the provisions of the Regulation, request additional information necessary to establish your identity.

The company will provide an answer to the respondent's request about the implementation without delay, and no later than within one month from the date of receipt of the request. This deadline can be extended by two additional months, taking into account the complexity and number of requests received.

The company will notify the respondent of any such extension within one month from of receiving the request, stating the reason for the extension.

If the Company does not act on the respondent's request, it will inform the respondent without delay, and no later than one month from the submission of the request, of the reasons for not acting and of the possibility of submitting a complaint to AZOP.

In accordance with the General Regulation, due to violation of the provisions, the competent authority for the protection of personal data can impose fines in the amount of up to 4% of the total annual turnover at the world level, or EUR 20 million.

2.12 Compliance with the General Regulation

The following actions are taken to ensure that the Company complies at all times with the principle established by the General Regulation:

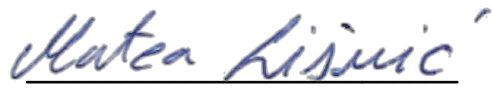
- the legal basis for processing personal data is clear and unambiguous;
- a personal data protection officer is appointed with specific responsibility for the protection of personal data in the organization (if necessary);
- all employees who participate in the handling of personal data understand their responsibilities regarding good practice in the protection of personal data;
- training in the field of personal data protection is provided to all employees;
- the rules on consents are respected;
- respondents who wish to exercise their rights regarding personal data are enabled to do so and such inquiries are dealt with efficiently;
- regular checks of procedures involving personal data are carried out;
- technical privacy protection is adopted for all new or modified systems and procedures;
- processing records are created with the following data:
 - organization name and relevant details;
 - purpose of personal data processing;
 - categories of individuals and personal data that are processed;
 - categories of recipients of personal data;
 - agreements and mechanisms for the transfer of personal data to countries outside the European Union, including details of existing checks;
 - duration of storage of personal data;
 - relevant technical and organizational controls carried out on site.

The aforementioned actions are regularly checked as part of the management process related to the protection of personal data.

2.13. Final provisions

This Privacy and Personal Data Protection Policy - GDPR internal act, enters into force on the date of its adoption, and applies from 01.07.2024. years.

MANAGEMENT OF THE COMPANY



Matea Lišnić



Raul Jimenez Vazquez