OLIMPIA

BICYCLE MANUFACTURING, TRADE AND SERVICES

LIMITED LIABILITY COMPANY

PRIVACY NOTICE AND DATA PROCESSING POLICY

Specific activity:

Bicycle design, assembly and sales.

Headquarters:

1164 BUDAPEST, Ostorhegy utca 4.

Located at:

1172 BUDAPEST, Lokátor utca 6.

Company register number: 01-09-566339

Tax number: 12216109-2-42

List of contents:

Created by: Zádori Tibor Data Protection Officer
e-mail: gdpradatvedelmiszabalyzat@gmail.com

Start of validity of this document: 2023.12.18.
Due date for review: Until the change in data management, but no later than December 2024.

Application of the Privacy and Data Protection Policy

Name of the organisation:	Olimpia Kerékpár Kft.
Headquarters of the organisation:	1164 BUDAPEST, Ostorhegy utca 4.
Person responsible for the content of the Code:	C. Szabó Péter
Date of entry into force of these rules:	2023.12.18.

This policy sets out rules on the protection of natural persons with regard to the processing of personal data and on the free flow of personal data. It shall apply to specific processing activities and to the issuing of instructions and notices governing the processing.

The obligation to employ (designate) a data protection officer extends to all public authorities or other bodies with a public-service mission (regardless of the data they process) and other organisations whose main activity is the systematic, large-scale monitoring of individuals or which process large numbers of special categories of personal data.

The organisation shall appoint a Data Protection Officer ☐ apply X does not apply

If a Data Protection Officer is employed:

Name:	
His position is:	
Contact:	

Scope of the Code

This policy is valid until revoked and applies to the officers, employees and Data Protection Officer of the organisation.

Date: 2023.12.18

.....
head of the organisation

Purpose of the Code

The purpose of this Policy is to harmonise the requirements of the other internal rules of the organisation with regard to data management activities in order to protect the fundamental rights and freedoms of natural persons and to ensure the adequate processing of personal data.

The organisation aims to comply fully with the legal requirements for the processing of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council.

A further important purpose of issuing the Code is to ensure that by knowing and complying with it, employees of the organisation are able to handle the data of natural persons lawfully.

Key concepts, definitions

- the **GDPR** (General Data Protection Regulation) is the new EU Data Protection Regulation

- **controller**: the natural or legal person, public authority, agency or any 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 the processing are determined by Union or Member State law, the controller or the specific criteria for the controller's designation may also be determined by Union or Member State law;

- **processing**: 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, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **processor**: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

- **personal data**: any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- **third party**: a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct authority of the controller or processor, are authorised to process personal data;

- **data subject's consent**: a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she signifies, by a statement or by an act expressing his or her unambiguous consent, that he or she signifies his or her agreement to the processing of personal data concerning him or her;

- **limitation of processing**: the marking of stored personal data for the purpose of limiting their future processing;

- **pseudonymisation**: the processing of personal data in such a way that it is no longer possible to identify the natural person to whom the personal data relate without further information, provided that such further information is kept separately and technical and organisational measures are taken to ensure that no link can be established between the personal data and identified or identifiable natural persons;

- **filing system**: a set of personal data structured in any way, whether centralised, decentralised or structured according to functional or geographical criteria, which is accessible on the basis of specific criteria;

- **data breach**: a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Guidelines for data management

The processing of personal data must be lawful, fair and transparent for the data subject.
A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet.

The purposes for which personal data are processed must be adequate, relevant and limited to what is necessary.

Personal data must be accurate and up to date. Inaccurate personal data must be deleted without delay.

Personal data must be stored in a form which permits identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods only if the storage is for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes.

Personal data must be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical or organisational measures.

The data protection principles apply to any information relating to an identified or identifiable natural person.

An employee of the organisation who is responsible for data processing is liable to disciplinary action, compensation, civil and criminal liability for the lawful processing of personal data. If an employee becomes aware that personal data he or she is processing is inaccurate, incomplete or out of date, he or she must correct it or have it corrected by the person responsible for recording it.

Processing of personal data

Because natural persons can be associated with online identifiers, such as IP addresses and cookie identifiers, provided by the devices, applications, tools and protocols they use, this data, combined with other information, can and may be used to profile and identify natural persons.

Processing may only take place if the data subject gives his or her freely given, specific, informed and unambiguous consent to the processing of the data by means of a clear affirmative action, such as a written, including electronic, or oral statement.

Consent to the processing of personal data is also deemed to be given if the data subject ticks a box to this effect when viewing the website. Silence, ticking a box or inaction does not constitute consent.

Consent shall also be deemed to be given when a user, in the course of using electronic services, makes the relevant technical settings or makes a statement or takes an action which, in the relevant context, clearly indicates the consent of the person concerned to the processing of his or her personal data.

Personal data concerning health include data relating to the health of a data subject which contains information about his or her past, present or future physical or mental health. This includes:

- registration for health services;

- a number, symbol or data assigned to an individual for the purpose of identifying that individual for health purposes;

- information obtained from the testing or examination of a body part or constituent material, including genetic data and biological samples;

- information about the person's illness, disability, disease risk, medical history, clinical treatment or physiological or biomedical condition, regardless of its source, which may be, for example, a doctor or other health professional, hospital, medical device or diagnostic test.

Genetic data shall be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person and resulting from the analysis of a biological sample taken from that person, in particular chromosomal analysis or analysis of deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) or any other element allowing the extraction of information equivalent to that which may be obtained from them.

Children's personal data deserve special protection, as they may be less aware of the risks, consequences, safeguards and rights associated with the processing of personal data. This special protection should apply in particular to the use of children's personal data for marketing purposes or for the purpose of creating personal or user profiles.

Personal data must be processed in a manner that ensures an adequate level of security and confidentiality, inter alia, in order to prevent unauthorised access to and use of personal data and the means used to process personal data.

All reasonable steps must be taken to correct or delete inaccurate personal data.

Lawfulness of data processing

The processing of personal data is lawful if one of the following conditions is met:

- you have given your consent to the processing of your personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject prior to entering into the contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary for the protection of 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;
- the 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.

As set out above, processing is lawful if it is necessary in the context of a contract or the intention to conclude a contract.

Where the processing is carried out in the performance of a legal obligation to which the controller is subject or where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing must have a legal basis in Union law or the law of a Member State.

Processing shall be regarded as lawful when it is carried out for the purpose of protecting the life of the data subject or the interests of another natural person mentioned above. Personal data processing based on the vital interests of another natural person should, in principle, only take place if there is no other legal basis for the processing in question.

Some types of personal data processing may serve both important public interests and the vital interests of the data subject, for example where the processing is necessary for humanitarian reasons, including when it is necessary to monitor epidemics and their spread, or in the event of a humanitarian emergency, in particular a natural or man-made disaster.

The legitimate interests of the controller, including the controller with whom the personal data may be shared, or a third party may provide a legal basis for the processing. Such legitimate interest may be, for example, where there is a relevant and appropriate relationship between the data subject and the controller, such as where the data subject is a client or employee of the controller.

The processing of personal data strictly necessary for the prevention of fraud is also considered to be in the legitimate interest of the controller concerned. Processing of personal data for direct marketing purposes may also be considered to be based on legitimate interest.

In order to establish the existence of a legitimate interest, it is necessary to carefully assess, inter alia, whether the data subject could reasonably expect, at the time and in the context of the collection of the personal data, that processing for the purposes for which the data were collected would take place. The interests and fundamental rights of the data subject may prevail over the interests of the controller where personal data are processed in circumstances in which the data subjects do not expect further processing.

The processing of personal data by public authorities, cyber emergency response units, network security incident management units, operators of electronic communications networks and service providers and security technology service providers to the extent strictly necessary and proportionate to ensure network and information security is considered to be in the legitimate interest of the controller concerned.
The processing of personal data for purposes other than those for which they were originally collected is permitted only if the processing is compatible with the original purposes for which the personal data were originally collected. In this case, a separate legal basis other than the legal basis which made the collection of the personal data possible is not necessary.

The processing of personal data by public authorities in order to achieve the purposes of officially recognised religious organisations, as defined by constitutional law or public international law, is considered to be in the public interest.

Consent of the data subject, conditions

- Where processing is based on consent, the controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data.

- Where the data subject gives his or her consent in the context of a written declaration which also relates to other matters, the request for consent must be communicated in a manner clearly distinguishable from those other matters.

- The data subject has the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent prior to its withdrawal. The data subject shall be informed before consent is given. The withdrawal of consent shall be made possible in the same simple manner as the giving of consent.

- In determining whether the consent is voluntary, the utmost account should be taken of the fact, inter alia, whether the performance of the contract, including the provision of services, is made conditional on consent to the processing of personal data which are not necessary for the performance of the contract.

- The processing of personal data in relation to information society services offered directly to children is lawful when the child is at least 16 years old. In the case of children under the age of 16, the processing of personal data of children is lawful only if and to the extent that consent has been given or authorised by the person having parental authority over the child.

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic data or biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons shall be prohibited, unless the data subject has given his or her explicit consent to the processing of those personal data for one or more specific purposes.

The processing of personal data relating to decisions on criminal liability and to criminal offences and related security measures may only take place if it is carried out by a public authority.

Processing that does not require identification

If the purposes for which the controller processes the
personal data do not or no longer require the identification of the data subject by the controller, the controller is not obliged to retain additional information.

Where the controller can demonstrate that it is not in a position to identify the data subject, it shall, as far as possible, inform the data subject accordingly by appropriate means.

Information and rights of the data subject

The principle of fair and transparent processing requires that the data subject be informed of the fact and purposes of the processing.

Where personal data are collected from the data subject, the data subject must also be informed of the obligation to provide the personal data and of the consequences of not providing the data. This information may also be supplemented by standardised icons to provide the data subject with general information about the envisaged processing in a prominent, easily understandable and clearly legible form.

Information relating to the processing of personal data concerning the data subject must be provided to the data subject at the time of collection or, where the data have been collected from another source than the data subject, within a reasonable period, having regard to the circumstances of the case.

The data subject shall have the right of access to the data collected concerning him or her and the right to exercise this right simply and at reasonable intervals in order to ascertain and verify the lawfulness of the processing. Each data subject should have the right to be informed, in particular, of the purposes for which personal data are processed and, where possible, the period for which the personal data are processed.

In particular, the data subject has the right to have his or her personal data erased and no longer processed if the collection or other processing of the personal data is no longer necessary in relation to the original purposes of the processing or if the data subjects have withdrawn their consent to the processing of the data.

Where personal data are processed for direct marketing purposes, the data subject should have the right to object, free of charge and at any time, to the processing of personal data concerning him or her for such purposes.

Review of personal data

In order to ensure that the storage of personal data is limited to the necessary period, the controller shall set time limits for erasure or periodic review.

Periodic review period set by the head of the organisation: 1 year.

Tasks of the data controller

The controller shall apply appropriate internal data protection rules to ensure lawful processing. These rules cover the powers and responsibilities of the controller.

The controller has the obligation to implement appropriate and effective measures and to be able to demonstrate that the processing activities comply with the applicable law.

This should be done taking into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

The data controller shall implement appropriate technical and organisational measures, taking into account the nature, scope, context and purposes of the processing and the varying degrees of risk to the rights and freedoms of natural persons, which vary in likelihood and severity. It shall review and, where necessary, update other internal rules on the basis of these rules.

The controller or processor shall keep adequate records of the processing activities carried out under its authority. Each controller and processor shall cooperate with the supervisory authority and make these records available on request in order to monitor the processing operations concerned.

Rights in relation to data processing

The right to request information

Any person may request information, through the contact details provided, about what data the organisation processes, on what legal basis, for what purpose, from what source and for how long. The request will be sent to the contact details provided without undue delay and within 30 days at the latest.

The right to rectification

Any person may request a change to any of their details using the contact details provided. Such a request shall be acted upon promptly and within 30 days at the latest and information shall be sent to the contact details provided.

The right to erasure

Any person may request the deletion of their data by using the contact details provided. Upon request, this must be done without undue delay and within 30 days at the latest, and information must be sent to the contact details provided.

Right to blocking, restriction

Any person can request the blocking of their data by using the contact details provided. The blocking will last as long as the reason stated makes it necessary to store the data. Upon request, this must be done without delay and within a maximum of 30 days and information must be sent to the contact details provided.

The right to protest

Any person may object to the processing of their data using the contact details provided. The objection shall be examined and a decision shall be taken on its merits within the shortest possible time from the date of the request, but not later than 15 days, and information on the decision shall be sent to the contact details provided.

Enforceability of data processing

National Authority for Data Protection and Freedom of Information
Postal address: 1530 Budapest, Pf.: 5.
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu
URL https://naih.hu
coordinates: N 47°30'56''; E 18°59'57''

In the event of a breach of the data subject's rights, the data subject may take the controller to court. The court shall rule on the case out of turn. The data subject may, at his or her option, bring the action before the competent court in the place where he or she resides or is domiciled.

The tasks of the organisation to ensure adequate data protection

- Data protection awareness. Ensure professional competence to comply with the law. Staff training and awareness of the rules is essential.

- The purpose of data processing, the criteria and the concept of personal data processing should be reviewed. Ensure lawful processing and processing in accordance with the data protection and data management policy.

- Proper information of the data subject. Attention should be paid to the fact that - where processing is based on the data subject's consent - in case of doubt, the controller must prove that the data subject has given his or her.

- The information provided to the data subject should be concise, easily accessible and easy to understand, and should therefore be drafted and presented in clear and plain language.

- Transparent processing requires that the data subject is informed of the fact and purposes of the processing. The information must be provided before the processing starts and the right to be informed during the processing until the processing ceases.

- The main rights of the data subject are:
    - access to personal data concerning him or her;
    - rectification of personal data;
    - erasure of personal data;
    - restrictions on the processing of personal data;
    - object to profiling and automated processing;
    - the right to data portability.

- The controller shall inform the data subject without undue delay and at the latest within one month of receipt of the request. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The obligation to provide information can be ensured by the operation of a secure online system through which the data subject can easily and quickly access the necessary information.

- Review the organisation's data management, ensure the right to information self-determination. At the request of the data subject, data must be deleted without delay if the data subject withdraws the consent on the basis of which the processing was carried out.

- The data subject's consent must unambiguously indicate that the data subject consents to the processing. Where the processing is based on the data subject's consent, the controller should, in case of doubt, prove that the data subject has consented to the processing operation.

- When processing personal data of children, particular attention should be paid to compliance with the rules on data processing. The processing of personal data in relation to information society services offered directly to children is lawful when the child is at least 16 years old. In the case of children under the age of 16, the processing of personal data of children is lawful only if and to the extent that consent has been given or authorised by the person having parental authority over the child.

- In the event of unlawful processing or processing of personal data, the supervisory authority must be notified. The controller must make the notification to the supervisory authority without undue delay and, if possible, no later than 72 hours after becoming aware of the personal data breach, unless the personal data breach is unlikely to pose a risk to the rights of the natural person.

- In certain cases, it may be appropriate for the controller to carry out a data protection impact assessment prior to processing. The impact assessment should assess the impact of the envisaged processing operations on the protection of personal data. If the DIA concludes that the processing is likely to present a high risk, the controller should consult the supervisory authority before processing personal data.

- Where the main activities involve processing operations which, by their nature, scope or purposes, require systematic and systematic large-scale monitoring of data subjects, a data protection officer should be appointed. The appointment of the DPO should aim at strengthening data security.

Data security

In particular, appropriate measures shall be taken to protect the data against unauthorised access, alteration, disclosure, disclosure, erasure or destruction, accidental destruction or accidental damage and against inaccessibility resulting from changes in the technology used.

To protect the electronically managed data files in the registers, appropriate technical arrangements should be in place to ensure that data stored in the registers cannot be directly linked and attributed to the data subject.

When designing and implementing data security, the state of the art must be taken into account. A choice should be made between several possible data processing solutions which ensure a higher level of protection of personal data, unless this would impose a disproportionate burden on the controller adatbiztonság megtervezésekor.

Data Protection Officer

The appointment of a Data Protection Officer is mandatory based on the following criteria:

- processing is carried out by public authorities or other bodies with public-service mission, except courts acting in their judicial role;

- the main activities of the controller or processor involve processing operations which, by their nature, scope or purposes, require systematic and systematic large-scale monitoring of data subjects;

- the main activities of the controller or processor concern the processing of a large number of personal data relating to decisions on criminal liability and criminal offences.

Where the appointment of a DPO is mandatory, the following rules apply:

The Data Protection Officer shall be appointed on the basis of his or her professional competence and, in particular, expert knowledge of data protection law and practice and his or her ability to perform the tasks of data controller.

The DPO may be an employee of the controller or the processor, but may also perform his or her tasks under a service contract.

The name and contact details of the data protection officer must be published by the controller or processor and communicated to the supervisory authority.

Status of the Data Protection Officer

The controller must ensure that the DPO is involved in all matters relating to the protection of personal data in an appropriate and timely manner. Ensure that the necessary resources are available to maintain the DPO's level of expertise.

The DPO shall not accept instructions from anyone in connection with the performance of his or her duties. The controller or processor shall not dismiss or sanction the DPO in connection with the performance of his or her duties. The DPO shall be directly responsible to the top management of the controller or processor.

Data subjects can contact the Data Protection Officer for all matters relating to the processing of their personal data and the exercise of their rights.

In the performance of his or her duties, the DPO shall be bound by an obligation of confidentiality or a duty of care.

The DPO may perform other tasks, but there should be no conflict of interest in relation to those tasks.

Tasks of the Data Protection Officer

- Provide information and professional advice to the controller or processor and to the staff carrying out the processing;
- monitor compliance with the controller's or processor's internal rules on the protection of personal data;
- on request, provide technical advice on the data protection impact assessment and monitor the conduct of the impact assessment;
- cooperate with the supervisory authority.

Data protection incident

A personal data breach is a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A data breach may cause physical, pecuniary or non-pecuniary damage to natural persons, including loss of control over their personal data or restriction of their rights, discrimination, identity theft or misuse of their identity, if not addressed in an appropriate and timely manner.

A data protection incident must be notified to the competent supervisory authority without undue delay and within 72 hours at the latest, unless it can be demonstrated, in accordance with the principle of accountability, that the data protection incident is unlikely to pose a risk to the rights and freedoms of natural persons.

The data subject must be informed without delay if the personal data breach is likely to result in a high risk to the rights and freedoms of the natural person, in order to enable him or her to take the necessary precautions.

Processing for administrative and record keeping purposes

The organisation may also process personal data in connection with its activities and for administrative and record-keeping purposes.

The processing is based on the freely given and explicit consent of the data subject, based on appropriate information. After detailed information, including the purposes, legal basis and duration of the processing and the rights of the data subject, the data subject must be made aware of the voluntary nature of the processing. Consent to the processing shall be recorded in writing.

Data processing for administrative and record-keeping purposes serves the following purposes:

- data processing of the organisation's members and employees based on a legal obligation;

- the processing of data of persons who have a contractual relationship with the organisation for contact, accounting and record-keeping purposes;

- contact details of other organisations, institutions and undertakings doing business with the organisation, which may include contact details and identification data of natural persons

The processing of data as described above is based on a legal obligation, on the one hand, and on the other hand, the data subject has given his or her explicit consent to the processing of his or her data (e.g. for the purposes of an employment contract or when registering as a partner on a website, etc.)

In the case of written documents (such as CVs, job applications, other submissions, etc.) containing personal data, the consent of the person concerned must be presumed. Once the case is closed, the documents should be destroyed in the absence of consent for further use. The fact of destruction shall be recorded in a report.

In the case of processing for administrative purposes, personal data are only included in the files and records of the case. The processing of these data lasts until the document on which the processing is based is disposed of.

Data processing for administrative and record-keeping purposes should be reviewed annually to ensure that the storage of personal data is limited to the necessary period, and inaccurate personal data should be deleted without delay.

Compliance with the law must also be ensured for processing for administrative and record-keeping purposes.

Processing for other purposes

If the organisation wishes to carry out a processing activity that is not covered by this policy, it must first supplement this internal policy accordingly or add sub-policies that are appropriate to the new processing purpose.

Other documents related to the Code

Documents and policies that contain, for example, a written statement of consent to data processing or, in the case of websites, a mandatory privacy notice, should be linked to and managed together with the privacy and data protection policy.

Laws on which the processing is based

- REGULATION (EU) No 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 Regulation (EC) No 95/46/EC (General Data Protection Regulation).

- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.

- Act LXVI of 1995 on public records, public archives and the protection of private archival material.

- Government Decree 335/2005 (XII. 29.) on the general requirements for document management by public bodies.

- Act CVIII of 2001 on certain aspects of electronic commerce services and information society services.

- Act C of 2003 on electronic communications.

Information on data management

for the processing of personal data by the National Authority for Data Protection and Freedom of Information in the context of public authority procedures for the protection of personal data and the enforcement of requirements concerning the protection of public interest or public access to data

1. Name and contact details of the Data Controller

National Authority for Data Protection and Freedom of Information (hereinafter "the Authority")
Headquarters: 1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1363 Budapest, Pf. 9.
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mail address: ugyfelszolgalat@naih.hu

2. Name and contact details of the Data Protection Officer

Data Protection Officer of the Authority: dr. Attila Kiss
Direct contact details: e-mail address: dpo@naih.hu; telephone number: +36 (1) 391-1470

3. Purpose of data processing

The purpose of the processing is to comply with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council[1] (hereinafter: GDPR) 57 and 58 of the GDPR in relation to the enforcement by the Authority of the requirements of the protection of personal data and the access to data of public interest or in the public interest. and the exercise of the following tasks and competences pursuant to Article 38(2) of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter: Infotv) and the following tasks and competences pursuant to Article 38(3) of the Infotv:

- conducting an investigation procedure on the basis of a notification or ex officio (Infotv. § 51/A-59);
- at the request of the data subject and ex officio, to conduct a procedure before a data protection authority (Infotv. 60-61. §);
- conducting ex officio confidentiality supervision proceedings (Infotv. § 62-63);
- conducting a data processing authorisation procedure upon request (Infotv. § 64/A-64/D);
- intervention in a court or in a lawsuit brought by another person for infringement of data of public interest and data in the public interest (Infotv. 64. §);
- in connection with the foregoing activities, international cooperation pursuant to Articles 65-68 of the Data Protection Act and Articles 60-65 of the General Data Protection Regulation.

After the completion of the cases under each procedure, the management of the data is governed by Act LXVI of 1995 on public records, public archives and the protection of private archival material (hereinafter: Ltv.) 2

1 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

in accordance with the rules - for archiving purposes in the public interest, scientific and historical research purposes and statistical purposes, subject to Article 89 of the GDPR.

4. Legal basis for processing

The processing is based on Article 6 (1) (e) GDPR, with regard to the tasks and competences pursuant to Articles 56-58 GDPR and Infotv 38 and 51/A-68 of the Information Act. The processing of data in connection with the performance of these tasks and the exercise of these competences shall be carried out taking into account the following legal provisions:

- Section 71 of the Information Act (the Authority shall process, to the extent and for the duration necessary for the conduct of its proceedings, all personal data and data classified as legally protected secrets and professional secrets which are related to the proceedings or the processing of which is necessary for the effective conduct of the proceedings);
- in relation to public authority procedures, Section 27 and Sections 33-34 of Act CL of 2016 on General Administrative Procedure (hereinafter: Ákr.);
- Ltv. 4. § és 9. §;
- in the case of procedures involving the processing of classified data, Articles 10 and 13 of Act CLV of 2009 on the Protection of Classified Data (hereinafter: Mavtv.).
- In the case of processing of special categories of data, where the special categories of data are not brought to the attention of the Authority by the data subject, the processing is also based on.
- in the case of a procedure based on a request or notification, Article 9(2)(f) of the GDPR,
- in the case of ex officio proceedings, Article 9(2)(g).

The categories of data subjects are: applicants, whistleblowers, complainants, other clients and other participants in official proceedings, natural persons consulted in the course of an investigation procedure in the context of the processing of personal data which is the subject of the procedure, data subjects of personal data examined or obtained in the course of clarifying the facts.

5. Scope and source of the data processed, if not provided to the Authority by the data subject

- **Natural person identification data** of the customer and other participants in the procedure, if not provided to the Authority by the customer;
- Depending on the nature and subject matter of the case**, other personal data necessary to clarify the facts of the case**, **including personal data of persons who are vulnerable persons** for the purposes of the GDPR, and **special categories** of personal data within the meaning of Article 9(1) of the GDPR and **personal data concerning criminal matters** as defined in Article 10 of the GDPR.

Personal data may come to the attention of the Authority from the following sources, provided that they have not been provided to the Authority by the data subject:

- **Data subject:** in addition to the personal data necessary to identify the person initiating the Authority's procedure, the Authority also processes personal data voluntarily provided by the data subject;
- **The register of personal data and addresses held by the Ministry of the Interior:** if your declaration is necessary for the effective conduct of a procedure of the Authority, but you are not available at the contact address of the Authority, the Authority may request information from the register of personal data and addresses;
- **Register of administrative records:** the Register of administrative records is used to electronically register and record a citizen's administrative declarations (e.g. authorisations, official contact details) and to allow access to this information by the authorised bodies, facilitating citizens' daily administration. The Authority, as a public administration body obliged to administer public affairs electronically, is obliged to electronically retrieve the information stored in the register of the customer's administrative disposition in accordance with Article 23 of Government Decree 451/2016 (XII. 19.) on the detailed rules of electronic administration. In order to make such a query, the Authority must know the natural identity of the customer.
- **Data controller or processor subject to the procedure:**
    - the Authority may need information about which personal data are processed by the controller in order to carry out its procedure. In such cases, it may request the controller to provide information about those data or to send copies of documents containing personal data to the Authority.
    - in the course of proceedings, the Authority may copy all or part of the records kept by data controllers, or make copies of or seize personal data media in order to clarify the facts and to ensure the effective conduct of the proceedings;
- **Other persons requested, other participants in the procedure:** in order to establish the facts, the authority may request information from the persons or bodies requested to the extent necessary, including.
    - process personal data necessary for the identification of the person involved in the procedure (client, representative, witness, owner of the object of inspection, other respondent),
    - personal data contained in evidence (data media) which he or she has provided voluntarily or at the Authority's request;
- **Other Member State data protection authority:** if the complaint about the processing is not lodged in Hungary, but the controller has its head office or a single place of business in Hungary and the decision about the processing complained of was taken at the controller's head office or single place of business, the Authority will act as the primary authority. In such a case, the authority where the complaint was lodged will send the Authority the documents and information necessary for the conduct of its proceedings, including the personal data provided to it.
- **Judicial enforcement:** where the Authority applies for judicial enforcement to the National Court Registry (see point 6.3 of this notice**)**

- upon receipt and acknowledgement of the application for an enforcement order by the court issuing the enforcement order, the Authority will manage the court enforcement case number;

- after the court has ordered the enforcement, the Hungarian Court Enforcement Chamber appoints the acting bailiff, who will provide the bailiff's case number at the first contact. The Authority will also process this data.

If the judicial enforcement is unsuccessful, the executor shall also inform the Authority of the outcome of each enforcement action: if the debtor has no enforceable assets, the fact of this, and if the debtor has enforceable assets, the context of the enforcement (e.g. location of the property, the parcel number, the debtor's share of ownership, whether the collection of the debtor's bank accounts was successful).

6. The recipients or categories of recipients of personal data

6.1. In relation to the processing of personal data contained in the documents on file:

- **Magyar Nemzeti Levéltár** (Postal address: 1250 Budapest, Pf. 3.; address: 1014 Budapest, Bécsi kapu tér 2-4.) (hereinafter: MNL): the Authority's records management rules and archive plan provide for the transfer of the records of cases that cannot be scrapped to MNL.
- **NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (**1081 Budapest, Csokonai u. 3. Postal address: 1389 Budapest, Pf. 133.): as the operator of the Registry.

6.2. In relation to the disclosure of documents, with regard to the data required for that purpose, taking into account any declaration made by the client in the Register of Case-files:

- **Magyar Posta Zrt.** (head office: 1138 Budapest, Dunavirág utca 2-6.): the Authority will provide it with data in the course of the procedure in question in the context of its contacts with customers.
- **NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.** (1081 Budapest, Csokonai u. 3. Postal address: 1389 Budapest, Pf. 133.): in the context of electronic communication with customers (in the case of regulated and centralised electronic administration services, for example the provision of the Authority's gateway)
- **KOPINT-DATORG Informatikai és Vagyonkezelő Kft.** (1081 Budapest, Csokonai u. 3. Postal address: 1428 Budapest Pf. 12.) in the framework of electronic communication with customers (for certain regulated and central electronic administration services)
- **DotRoll Kft.** (1148 Budapest, Fogarasi út 3-5.): is involved as the data processor of the mail system for the data transmitted by the Authority through its electronic mail system

6.3. In addition, the Authority will only exceptionally, in a specific case, communicate personal data processed in the context of its procedures to other bodies which are not recipients within the meaning of Article 4(9) of the GDPR, for the purposes of its own or another body's public authority procedures. Such bodies may typically include:

- **Client in data protection/privacy proceedings:** in exercising his right of access to the file, he may have access to unclassified personal data, as required by law. With regard to classified data, the rules on access are governed by the provisions of the Act on the Protection of Classified Data, according to which the classifier is entitled to grant access authorisations[2] to the data subject.

- **Bodies, persons and supervisory authorities consulted in the course of the procedure:** where other authorities, bodies or persons consulted in the course of the procedure are necessary to clarify the facts or take a decision, the Authority may disclose personal data to the extent strictly necessary to comply with the request.

- with the requested Hungarian authority, body, person or supervisory authority of another EU Member State under the GDPR,

- in proceedings under Articles 56 and 60 to 65 of the GDPR with the supervisory authority of another EU Member State, the European Data Protection Board (the Board), the Board's Secretariat and the Commission of the European,

- the controller, processor or recipient of the data transfer being investigated in the procedure;

- other requested body, person.

- **Other Hungarian authority with competence and jurisdiction:** if the processing of an application received by the Authority falls within the competence of another authority, the Authority shall refer the case containing personal data to that authority pursuant to Section 17 of the General Civil Code.

- **Courts:** the court hearing a case relating to the administrative activities of the Authority or a case brought by the Authority pursuant to Article 64 of the Information Act may access and process personal data contained in the case file in accordance with the procedural rules applicable to the case. In administrative proceedings against the decisions of the Authority, the Authority shall submit the documents of the administrative case to the court together with the statement of claim submitted to it pursuant to Section 40(1) of Act I of 2017 on the Code of Administrative Procedure (hereinafter referred to as the "Kp").

- **The competent directorate of the National Tax and Customs Administration (hereinafter: NAV):** if the customer has not complied with the obligation to pay the money - procedural or data protection fine, procedural costs - set out in the final decision of the Authority in the data protection authority procedure, and the Authority orders enforcement, the Authority shall apply to the NAV for the recovery of the money claim pursuant to Section 134 (1) of the General Tax Code and Section 61 (7) of the Information Act. To the extent and within the scope necessary to comply with this request, the Authority shall, where appropriate, transmit personal data to the NAV.

- **National Office of the Courts (OBH):** according to § 1 of Act LIII of 1994 on Judicial Enforcement, the decisions of courts and other bodies deciding on disputes, as well as claims based on certain documents, are enforced by judicial enforcement in accordance with the Act. The Authority submits the application for judicial enforcement to the OBH. When submitting the application for enforcement, the Authority shall, pursuant to Section 11(2) of the Act, communicate to the OBH the following information:

    - 6 [2] According to § 11 of the Mavtv.

a) the name of the debtor (name in the case of an organisation, company name in the case of a company) and the data necessary to identify the debtor (at least the place and date of birth and the name of the mother or the registration number of the organisation, company registration number in the case of a company), and

b) depending on the circumstances of the case, the debtor's domicile, place of work, registered office or place of business (hereinafter referred to as "the registered office") and the location of the property subject to enforcement; at least one of the items of information listed in this point must be provided.

In addition to the above, the Authority shall communicate the following information to the OHI when submitting the request for enforcement: the number of the Authority's decision, the date, number and date of finality of the court decision, the amount and title of the claim to be enforced and the last day of the deadline for execution.
In the case of judicial enforcement, the enforcement shall be carried out by an independent bailiff.

– **Investigating authority**: if an investigating authority approaches the Authority and requests the transmission of documents for the purposes of an investigation, the Authority is obliged to provide them to the Authority together with the personal data contained therein. If, in the course of or in connection with the Authority's proceedings, a criminal offence or an infringement is suspected and the Authority therefore initiates criminal proceedings or infringement proceedings before the body entitled to initiate proceedings pursuant to Section 70 of the Information Act, it shall forward the file required for the filing of a complaint, together with the personal data contained therein, to the competent investigating authority**.**

7. Duration of storage of personal data

The Authority shall file the documents related to the case in accordance with the legal requirements for the management of documents of public bodies[3] and shall keep them among the filed documents until the date of their destruction as specified in the current archiving plan or, failing that, until their transfer to the archives. The Authority shall keep the data with the documents for archiving purposes until they are disposed of or archived. Thereafter, with the exception of the data contained in the documents to be archived pursuant to the Act and the personal data to be processed in the records management system pursuant to the law, the Authority shall delete the data (scrap the documents) or cease to process the personal data at the Authority upon archiving.

8. Rights of the data subject in relation to data processing

8.1. Deadline

The Authority shall comply with a request to exercise the rights of the data subject within one month of receipt of the request. The date of receipt of the request shall not count towards the time limit.

The Authority may, if necessary, and taking into account the complexity of the application and the number of applications, extend this period by a further two months. The Authority shall inform the person concerned of the extension, stating the reasons for the delay, within one month of receipt of the request.

3 Ltv., and Government Decree 335/2005 (XII. 29.) on the general requirements of document management of bodies performing public functions.

8.2. Data subjects' rights in relation to data processing

8.2.1. The right of access

The data subject shall have the right to obtain from the Authority, through the contact details provided under point 1, information as to whether or not his or her personal data are being processed and, if such processing is taking place, the right to be informed that:

- The Authority
- what personal data;
- on what legal basis;
- for what processing purpose;
- for how long

manages; and that,

- - to whom, when, on the basis of which law, to which personal data the Authority has granted access or to whom it has transferred personal data;
- the source of the personal data (if not provided to the Authority by the data subject);
- whether the Authority uses automated decision-making and its logic, including profiling.

The Authority shall provide the data subject with a copy of the personal data concerned free of charge for the first time upon request and may charge a reasonable fee based on administrative costs thereafter.

In order to meet data security requirements and to protect the rights of the data subject, the Authority is obliged to verify the identity of the data subject and of the person who wishes to exercise the right of access, and to this end, the provision of information, access to data and the issuing of copies of data are subject to the identification of the data subject.

In public authority proceedings, the rules of § 33-34 of the Ákr. apply to access to the case file.

8.2.2. The right to rectification

The data subject may request that the Authority amend any of his or her personal data by using the contact details provided in point 1. If the data subject can credibly demonstrate the accuracy of the corrected data, the Authority shall comply with the request within a maximum of one month and shall inform the data subject thereof using the contact details provided by the data subject..

8.2.3. The right to blocking (restriction of processing)

The data subject may request, through the contact details provided in point 1, that the Authority restricts the processing of his or her personal data (by clearly indicating the restriction and ensuring that the processing is kept separate from other data) where. contests the accuracy of his or her personal data (in which case the Authority will restrict the processing for the time necessary to verify the accuracy of the personal data);

- the data processing is unlawful and the data subject opposes the erasure of the data and instead requests the restriction of their use;

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

- the data subject has objected to the processing (in which case the restriction applies for the period until it is established whether the legitimate grounds of the controller override those of the data subject).

In addition to the above, in official proceedings, the Authority may, upon request or ex officio, order the confidential treatment of the natural identity and address of the client and other participants in the proceedings, if justified under Section 28 of the Ákr., if their cooperation in the proceedings may have serious negative consequences; Ákr. According to Article 30, the Authority may, in order to protect minors, incapacitated or partially incapacitated adults, witnesses, owners of evidence or persons under surveillance, decide to restrict the processing of data and the right of access to documents without a request to that effect.

8.2.4. The right to protest

The data subject may object to the processing of his or her personal data if he or she considers that the Authority is processing his or her personal data in a way that is incompatible with the purposes of this privacy notice, by using the contact details provided in point 1. In such a case, the Authority must demonstrate compelling legitimate grounds for the processing of the personal data which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

8.2.5. The right to erasure

The data subject may exercise his or her right to erasure in relation to the processing described in this notice only if the data are no longer necessary for the performance of a task carried out in the exercise of official authority vested in the Authority. With regard to the documents to be archived, the deletion of data cannot be achieved without affecting the integrity of the documents..

9. Right to legal redress

Where the data subject considers that the Authority has infringed the applicable data protection requirements in the processing of his or her personal data, the data subject may,

- may lodge a complaint with the Authority (National Authority for Data Protection and Freedom of Information, address: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf. 9, E-mail: ugyfelszolgalat@naih.hu, Website: www.naih.hu), or

- have the right to apply to the courts, which will rule on the matter out of turn, in order to protect your data. In such a case, you are free to choose whether to bring your action before the courts having jurisdiction for the place where you reside (permanent address) or stay (temporary address) or before the courts for the place where the Authority is established. You can find the court of the place of residence or domicile at https://birosag.hu/birosag-kereso. The competent court for the seat of the Authority is the Metropolitan Court of Budapest.

In the case of decisions taken by the Authority in the course of official proceedings, in particular decisions relating to access to documents, a special remedy may be available under the General Procedures Act (Chapter IX of the Ákr.).

Olimpia Kerékpár Kft.

Data management information

to companies and other organisations that have a contractual relationship with the organisation

Introduction

As a data controller, the organisation has contractual relationships with businesses and other organisations that contribute to the smooth running of the organisation. The organisation processes the personal data of the officers and employees of these organisations - the data subjects - that are strictly necessary for the purposes of the relationship.

As a data controller, the organisation aims to fully comply with the legal requirements for the processing of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council.

This privacy notice has been prepared pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of personal data of natural persons and on the free movement of such data, subject to the requirements of Act CXII of 2011 on the right to information self-determination and freedom of information.

The organisation processes the data of natural persons associated with it in accordance with the law and the principles set out in its internal rules. In compliance with its internal rules, the organisation's officers and employees process the data of natural persons lawfully.

The organisation attaches the utmost importance to respecting the right to informational self-determination of the persons associated with it, treats their personal data confidentially and observes all technical and organisational measures to guarantee the security of the data..

This privacy notice provides information to data subjects about the processing of their personal data.

Name and contact details of the controller:

Name of the organisation:	Olimpia Kerékpár Kft.
Address of the organisation:	1164 BUDAPEST, Ostorhegy utca 4.
Website name, address:	www.gepida.hu
Mailing address:	1164 BUDAPEST, Ostorhegy utca 4.
E-mail:	hr@gepida.hu
Telephone:	+36 30 2283876

Guidelines for data management

The data controller declares that it processes personal data in accordance with its processing policy and complies with the provisions of the applicable legislation, in particular with regard to:

- Process personal data lawfully and fairly and in a transparent manner for the data subject.

- Personal data are processed only for specified, explicit and legitimate purposes. The specific purpose in this case is to communicate with contractual partners.

- The legal basis for processing is the consent of the data subject or a legal obligation.

- The data subjects are the contact officers and employees of companies and other organisations that have a contractual relationship with the organisation.

- Duration of processing and erasure of data. The duration of data processing will always depend on the specific purpose of the user, but data must be deleted immediately once the original purpose has been achieved. The data subject may withdraw his or her consent to the processing at any time. If there is no legal obstacle to erasure, your data will be deleted.

- The data controller and its employees are entitled to access the data.

- The data subject may request the controller to access, rectify, erase or restrict the processing of personal data relating to him or her and may object to the processing of such personal data.

- The data subject may withdraw his or her consent at any time, but this shall not alter the lawfulness of the processing carried out on the basis of consent prior to the withdrawal.

- The person concerned may exercise the right to lodge a complaint with the supervisory authority.

- The data subject shall have the right to obtain, at his or her request and without undue delay, the rectification or integration by the controller of inaccurate personal data relating to him or her.

- The data subject shall have the right to obtain from the controller, at his or her request and without undue delay, the erasure of inaccurate personal data relating to him or her and the controller shall be obliged to erase personal data relating to him or her without undue delay, unless there is another legal basis for the processing.

- You can request the modification or deletion of your personal data by e-mail, telephone or letter using the contact details provided in this notice.

- Personal data are stored in paper and electronic form in such a way as to allow identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods only if the storage is for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes.

- The processing and adequate security of personal data is ensured through technical and organisational measures. Protection against unauthorised or unlawful processing, accidental loss, destruction or damage is ensured.

- The data protection principles apply to all information relating to an identified or identifiable natural person.

Scope of data processed	Purpose of data processing
Name	Identification, contact, registration.
Address	Identification, contact, registration.
Phone number	Required for contact purposes.
E-mail	Required for contact purposes.

For matters not covered by the Privacy Notice, the Privacy Policy and the underlying laws and regulations shall govern.

Name of organisation: Olimpia Kerékpár Kft.

Address of: 1164 BUDAPEST, Ostorhegy utca 4.

Consent form for data processing

to access and process personal data

Name/Company name: ……..……

Address/Place of residence: ……..……

Phone number, email: ……..……

I, the above named individual, hereby give my consent to the access and processing of my personal data for contact purposes.

To achieve the purpose of the processing, the data must be transferred to the following controller:

Name of organisation: ……..……. Located at: ……..…….

To transmit data ☐ I contribute ☐ I do not contribute

I agree that the controller may also use my data for the following purposes:

Purpose of use: ……. ☐ I contribute ☐ I do not contribute

The data controller declares that the duration of data processing, unless otherwise provided for by law, lasts until the purpose of the processing has been achieved..

I, the undersigned, acknowledge that my personal data may be disclosed to the officers and employees of the organisation requesting this declaration. I declare that I have been informed in detail about the purpose of the processing, my rights in relation to the processing, that I understand them and that I have given my consent voluntarily in order to achieve the purpose of the processing.

Date: ……

.....

Signature in company format

Company name: Olimpia Kerékpár Kft.
Headquarters: 1164 BUDAPEST, Ostorhegy utca 4.
Company registration number: 01-09-566339

Interest screening test

Subject:

It is necessary to carry out this balancing of interests test in order to determine whether the conditions of the General Data Protection Regulation (GDPR) are met in relation to the personal data that is the subject of this balancing of interests test.

During the balancing of interests test:

1. the legitimate interest in processing the personal data subject to the balancing of interests test is identified
2. the necessity of the processing is assessed
3. the interests and fundamental rights of the Data Subject in relation to the personal data(s) subject to the interest test are established
4. a comparison is made between the legitimate interests of the undertaking and the interests and fundamental rights of the Data Subject and on this basis it is determined whether the Data Subject's personal data can be processed.

1. The legitimate interest of the undertaking (controller)

- Purpose of the processing:

  The main purpose of an enterprise as a business company is to achieve an economic result related to its activity. The customers of the enterprise are natural or legal persons to whom goods are sold or services are provided. In order to serve customers flexibly and smoothly, it is necessary to maintain stocks. The continuous monitoring of stocks and the provision of services are essential for the economic operation of the business.

- Description of the legitimate interest of the controller:

  The company has a large amount of valuable fixed and rotating assets, and continuous camera surveillance of these assets is essential to protect against unauthorised intruders. Camera surveillance is also important for monitoring the quality of services and assessing the legitimacy of potential customer complaints, as well as establishing the authenticity of an accident at work.

Finding:

The use of a camera is essential to protect property and goods, to check the quality of services, to verify the authenticity of customer complaints and to investigate the facts of an accident at work.

2. Examination of the necessity of the processing

- Why is data processing necessary to achieve the purpose?

According to GDPR (47), the legal basis for processing is the legitimate interest of the controller, where there is a relevant and appropriate relationship between the controller and the data subjects. On this basis, at the time of collection, data subjects can reasonably expect that the processing will be carried out for the purposes for which the data are collected.

- Is there an alternative solution to achieve the objective?

  At the moment, the only real way to protect and monitor assets is through CCTV.

- What are the disadvantages for the company if the data are not processed?

  Possible damage to and theft of property, including fixed and rotating equipment and movable property, cannot be documented reliably without a camera system and would greatly hamper the possibility of recovery.

Finding: the business activity justifies the use of a CCTV surveillance system.

3. Interests and fundamental rights of the Data Subject

- The company's relationship with the Data Subjects (interested parties, contracted partners, etc.):

  The company employs workers in the course of its economic activities. Before hiring a worker, he or she is given detailed information about his or her job and the rules of employment. Data protection is discussed during this process.

- Reasonable expectations, interests, fundamental rights or freedoms of the Data Subject: The Data Subject has a fundamental interest in ensuring that his or her privacy is respected by data controllers, that he or she can exercise his or her right to control the processing of his or her personal data and to exercise his or her right to informational self-determination. 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 him or her or similarly significantly affects him or her.

- Positive and negative effects of the processing on the Data Subject: the processing has / has not (underline as appropriate) negative effects on the Data Subject.

Finding: on the basis of the above, the Data Controller has assessed and taken into account the interests and rights of the Data Subjects.

4. Comparison of the interests of the business and the Data Subject (why the processing is proportionate)

The Data Subjects are employees of the company. Their income and the payment of the associated public charges are guaranteed by the enterprise contract. The enterprise is able to bear these costs as long as its economic activity is profitable. Accordingly, the data management of the enterprise, in this case the continuous video monitoring of the stock of assets, is also in the interest of the Data Subjects.

5. The result of the interest balancing test:

Following the balancing of interests test, it has been determined that the interest of the controller in processing the personal data outweighs the interest of the Data Subject in the protection of his or her personal data. The processing does not constitute an unnecessary and disproportionate restriction on the interests, fundamental rights or freedoms of the Data Subject. The Data Subject is informed of the essential circumstances of the processing and of the rights to which he or she is entitled before the processing of personal data starts. The Data Subject may object to the processing!

The processing is based on the exact legal basis of the undertaking (f).

On the basis of the above, the use of CCTV is justified and can be legally applied

Information on data management

the

http://www.gepida.hu

website visitors and registered users.

Introduction

The service provider / data controller processes the data of persons registered on the website in the course of its operation, in order to provide them with an appropriate service.

The service provider intends to fully comply with the legal requirements for the processing of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council.

This Privacy Notice has been prepared pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of personal data of natural persons and on the free movement of such data, taking into account the content of Act CXII of 2011 on the right to information self-determination and freedom of information.

Name of service provider, data controller

Name / company name:	Olimpia Kerékpár Kft.
Headquarters:	1164 BUDAPEST, Ostorhegy utca 4.
Tax number:	122161109-2-42
Registration number (NAIH):	------
Website name, address:	www.gepida.hu
Contact details of the privacy notice:	1164 BUDAPEST, Ostorhegy utca 4.

Contact details of the controller

Name / company name:	Olimpia Kerékpár Kft.
Headquarters:	1164 BUDAPEST, Ostorhegy utca 4.
Mailing address:	1164 BUDAPEST, Ostorhegy utca 4.
E-mail:	recepcio@gepida.hu
Telephone:	+36 1 400-6065

Definitions

- the **GDPR** (General Data Protection Regulation) is the European Union's new Data Protection Regulation;

- **processing:** 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, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **processor:** a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

- **personal data:** any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- **controller:** the natural or legal person, public authority, agency or any 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 the processing are determined by Union or Member State law, the controller or the specific criteria for the controller's designation may also be determined by Union or Member State law;

- **data subject's consent:** a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she signifies, by a statement or by an act expressing his or her unambiguous consent, that he or she signifies his or her agreement to the processing of personal data concerning him or her;

- **data breach:** a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **recipient:** the natural or legal person, public authority, agency or any other body, whether or not a third party, to whom or with whom the personal data are disclosed. Public authorities that may have access to personal data in the context of an individual investigation in accordance with Union or Member

State law are not recipients; the processing of those data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing;

- **third party:** a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Guidelines for data management

The data controller declares that it will process personal data in accordance with the provisions of the Privacy Notice and will comply with the applicable laws, in particular with regard to:

The processing of personal data must be lawful, fair and transparent for the data subject.

Personal data may only be collected for specified, explicit and legitimate purposes.

The purposes for which personal data are processed must be adequate, relevant and limited to what is necessary.

Personal data must be accurate and up to date. Inaccurate personal data must be deleted without delay.

Personal data must be stored in a form which permits identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods only if the storage is for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes.

Personal data must be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical or organisational measures.

The data protection principles apply to any information relating to an identified or identifiable natural person.

Important data management information

The purpose of data processing is to enable the service provider / data controller to provide additional services to the persons registered on the website.

The legal basis for processing is the consent of the person concerned.

The data subjects are the registration users of the website.

Duration of processing and erasure of data. The duration of data processing will always depend on the specific purpose of the user, but data must be deleted immediately once the original purpose has been achieved. The data subject may withdraw his or her consent to the processing at any time by sending an e-mail to the contact e-mail address. If there is no legal obstacle to the deletion, your data will be deleted.

The controller and its employees are entitled to access the data.

The data subject may request the controller to access, rectify, erase or restrict the processing of personal data relating to him or her and may object to the processing of such personal data and the data subject's right to data portability.

The data subject may withdraw his or her consent at any time, but this shall not affect the lawfulness of the processing carried out on the basis of the consent prior to its withdrawal.

The person concerned may exercise the right to lodge a complaint with the supervisory authority.

If the data subject wishes to benefit from the registration, i.e. to use the services of the website, he or she must provide the requested personal data. The data subject is not obliged to provide personal data and will not suffer any disadvantage if he/she does not provide such data. However, it is not possible to use certain functions of the website without registration.

The data subject shall have the right to obtain from the controller, at his or her request and without undue delay, the rectification or integration of inaccurate personal data relating to him or her.

The data subject shall have the right to obtain from the controller, at his or her request and without undue delay, the erasure of inaccurate personal data relating to him or her, and the controller shall be obliged to erase personal data relating to him or her without undue delay, unless there is another legal basis for the processing.

Changes or deletion of personal data may be initiated by e-mail, telephone or letter using the contact details provided above.

Registration on the website

The purpose of the processing is to provide additional services and to contact you.

The legal basis for registration data processing is your consent.
The data subjects are the registration users of the website.

Duration of processing. Processing will continue until consent is withdrawn. You may withdraw your consent to the processing at any time by sending an e-mail to the following contact e-mail address.

The data will be deleted when consent to data processing is withdrawn. You can withdraw your consent to data processing at any time by sending an e-mail to the contact e-mail address.

The data controller and its employees are entitled to access the data.
Method of storage of data: electronic.

Changes or deletion of personal data may be initiated by e-mail, telephone or letter using the contact details provided above.

The provision of personal data is strictly necessary for identification in databases and contact purposes. The exact company name and address are required for invoicing, which is a legal obligation.

Scope of data processed	Specific purposes for which the data are processed
Name	Identification, contact, billing.
Company name	Identification, contact, billing.
Address	Identification, contact, billing.
E-mail	Identification, contact.
Telephone	Identification, contact.
Date of registration	Technical information operation.
IP address	Technical information operation.

The user can give his/her consent to the processing of his/her personal data by deliberately ticking the blank checkbox on the website.

As a data subject, you have the right to object to the processing of your personal data, in accordance with the procedure set out in the processing information detailed above and in this notice and the legislation described in this notice.

Place an order

The purpose of data processing is to provide additional services, contact, send confirmation e-mails. We will only be able to fulfil your order if you provide us with your contact and billing details, which are strictly necessary for contact and billing purposes.

The legal basis for processing is your consent. In the case of billing, the processing is based on a legal requirement.

The data subjects are the registration users of the website.

Duration of processing. Processing is carried out until consent is required by law or withdrawn. You may withdraw your consent to the processing at any time by sending an e-mail to the contact e-mail address.

The data will be deleted when consent to data processing is withdrawn. You can withdraw your consent to data processing at any time by sending an e-mail to the contact e-mail address. Billing data may be deleted as required by law.

The controller and its employees are entitled to access the data..

Data storage method: electronic.

Changes or deletion of personal data may be initiated by e-mail, telephone or letter using the contact details provided above.

Scope of data processed	Specific purposes for which the data are processed
Name	Identification, contact, billing.
Company name	Identification, contact, billing.
Address	Identification, contact, billing.
E-mail	Identification, contact.
Telephone	Identification, contact.
Ordered product details	Identification of the product.
Date of registration	Technical information operation.
IP address	Technical information operation.

The user can give his/her consent to the processing of his/her personal data by deliberately ticking the blank checkbox on the website.

The data subject may object to the processing of his or her personal data, in which respect he or she has the right to the procedure set out in the processing information detailed above and in this notice and the legislation described in this notice.

Setting up an account

The purpose of the processing is to issue and send an electronic invoice as an e-mail attachment.
The legal basis for the processing is mandatory processing based on law.

The data subjects are the service provider's customer partners.

Duration of processing. Processing is carried out until consent is required by law or withdrawn. You may withdraw your consent to the processing at any time by sending an e-mail to the contact e-mail address.

The data will be deleted when consent to data processing is withdrawn. You can withdraw your consent to data processing at any time by sending an e-mail to the contact e-mail address. Billing data may be deleted as required by law.

The data controller and its employees are entitled to access the data.
Method of storage of data: electronic.
Changes or deletion of account data can be initiated by e-mail, telephone or letter using the contact details given above.

Scope of data processed	Specific purposes for which the data are processed
Name	Identification, contact, billing.
Company name	Identification, contact, billing.
Address	Identification, contact, billing.
E-mail	Identification, contact.
Telephone	Identification, contact.
Tax number / tax identification number	Identifying the buyer.
Account details	Identification of the account.
Számlakiállítás időpontja	Technical information operation.

The user can give his/her consent to the processing of his/her personal data by deliberately ticking the blank checkbox on the website.

The data subject may object to the processing of his or her personal data, in which respect he or she has the right to the procedure set out in the processing information detailed above and in this notice and the legislation described in this notice.

Send newsletter

As the operator of this website, we declare that the information and descriptions published by us fully comply with the relevant legal provisions. We also declare that when subscribing to a newsletter, we are not in a position to verify the authenticity of the contact details or to establish whether the details provided relate to an individual or a company. Companies that contact us will be treated as a customer partner.

The purpose of data processing is to send you professional brochures, electronic messages containing advertising, information and newsletters, from which you can unsubscribe at any time without any consequences. You may also unsubscribe without any consequences if your business has ceased to exist, you have left the business or someone has provided us with your contact details.

The legal basis for processing is your consent. Please be informed that the user may give his/her prior and explicit consent to be contacted by the service provider with promotional offers, information and other mailings to the e-mail address provided at the time of registration. As a consequence, the user may consent to the processing of the necessary personal data by the service provider for this purpose.

Please note that if you wish to receive a newsletter from us, you must provide the necessary information. If you do not provide this information, we will not be able to send you a newsletter.

Duration of processing. Processing will continue until consent is withdrawn. You can withdraw your consent to the processing at any time by sending an e-mail to the contact e-mail address.

The data will be deleted when consent to data processing is withdrawn. You can withdraw your consent to data processing at any time by sending an e-mail to the contact e-mail address.

Consent can also be withdrawn by following the link in the newsletters sent.

The controller and its employees are entitled to access the data.

Data storage method: electronic.

Changes or deletion of data can be initiated by e-mail, telephone or letter using the contact details provided above.

The registration number of the controller:	NAIH-……

The data processor used:	http://.....

Scope of data processed	Specific purposes for which the data are processed
Name	Identification, contact.
E-mail	Identification, contact.
Date of subscription	Technical information operation.
IP address	Technical information operation.

Please note that neither the username nor the e-mail address need to contain any personally identifiable information. For example, it is not necessary for the username or e-mail address to contain your name. You are entirely free to choose whether to provide a username or an e-mail address that contains information that identifies you. The e-mail address, which is used to contact you, is absolutely necessary to ensure that any newsletter or professional information sent to you is received.

Cookies

Cookies are placed on the user's computer by the websites visited and contain information such as the site's settings or login status.

Cookies are therefore small files created by the websites you visit. They improve the user experience by saving browsing data. Cookies help the website to remember your website settings and offer you locally relevant content.

A small file (cookie) is sent by the provider's website to the website visitors' computer in order to establish the fact and time of the visit. The provider informs the website visitor of this.

The data subjects are the visitors of the website.
The purpose of data processing is to provide additional services, identification and tracking of visitors.

Legal basis for processing. The user's consent is not required if the use of cookies is strictly necessary for the service provider.

The scope of the data: unique identification number, time, configuration data.

Users have the option to delete cookies from their browsers at any time by going to Settings.

The data may be accessed by data controllers. By using cookies, no personal data is processed by the data controller.

Data storage method: electronic.

Social media sites

A social networking site is a media tool where the message is spread through social users. Social media uses the Internet and online publishing to transform users from content receivers to content editors.

Social media is the interface of web applications that hosts user-generated content, such as Facebook, Google+, Twitter, Pinterest, etc.

Social media can take the form of public speeches, presentations, demonstrations, product or service launches.

Social media information can take the form of forums, blog posts, images, video, audio, message boards, email messages, etc.

As set out above, the scope of the data processed may include, in addition to personal data, the user's public profile picture.

Data subjects: all registered users.

The purpose of data collection is to promote the website or a related website.

The legal basis for processing is the voluntary consent of the data subject.

Duration of data processing: according to the rules available on the relevant community site.

Deadline for deletion of data: according to the rules available on the relevant Community site.

Those entitled to access the data: according to the rules available on the relevant Community site.

Data processing rights: according to the rules available on the relevant Community site.

Data storage method: electronic.

It is important to note that when a user uploads or submits personal information, he or she is giving the social networking site operator worldwide a valid permission to store and use such content.
Therefore, it is very important to make sure that the user has full permission to disclose the information posted.

Google Analytics

Our website uses Google Analytics X use ☐ do not use

When using Google Analytics:

Google Analytics uses internal cookies to compile reports for its customers on the habits of website users.

On behalf of the website operator, Google will use this information to evaluate how users use the website. As an additional service, the website operator will compile reports on website activity for the website operator so that it can provide additional services.

Data is stored on Google's servers in encrypted format to make it more difficult and prevent misuse.

You can disable Google Analytics by. Quote from the page:
Site users who do not want Google Analytics to generate JavaScript reports about their data can install the Google Analytics browser add-on to disable it. The extension will prevent Google Analytics JavaScript (ga.js, analytics.js, and dc.js) from sending information to Google Analytics. The browser extension can be used in most recent browsers. The Google Analytics browser add-on does not prevent data from being sent to the website itself and other web analytics services..
https://support.google.com/analytics/answer/6004245?hl=hu

Google Privacy Policy: https://policies.google.com/privacy?hl=hu

More detailed information on the use and protection of data is available at the links above.

Data protection in detail:
https://static.googleusercontent.com/media/www.google.com/en//intl/hu/policies/privacy/google_privacy_policy_hu.pdf

Data controllers

Shared space provider:

Name / company name:	Brainsum Kft.
Headquarters:	1092 BUDAPEST, Ráday utca 5.
Telephone:	+36 30 3018406
E-mail:	info@brainsum.com

The data you provide is stored on a server operated by the hosting provider. Only our staff or the staff operating the server have access to the data, but they are all responsible for the security of the data.

Activity description: hosting, server services.

Purpose of data processing: to ensure the functioning of the website.

Data processed: personal data provided by the data subject

Duration of processing and time limit for deletion of data. Data processing until the end of the website's operation or in accordance with the contractual agreement between the website operator and the hosting provider. If necessary, the data subject may request the deletion of his/her data by contacting the hosting provider.

The legal basis for processing is the consent of the data subject or processing based on law.

Data controllers

Shared space provider:

Name / company name:	Gepida Online Kft.
Headquarters:	1164 Ostorhegy utca 4.
Telephone:	+3630 9 988 220
E-mail:	support@gepida.com

The data you provide is stored on a server operated by the hosting provider. Only our staff or the staff operating the server have access to the data, but they are all responsible for the security of the data.

Activity description: trade in bicycles and spare parts

Purpose of processing: trade

Data processed: personal data provided by the data subject

Duration of processing and time limit for deletion of data. Data processing until the end of the website's operation or in accordance with the contractual agreement between the website operator and the hosting provider. If necessary, the data subject may request the deletion of his/her data by contacting the hosting provider.

The legal basis for processing is the consent of the data subject or processing based on law.

Data controllers

Shared space provider:

Name / company name:	Gepida Kerékpár Kft.
Headquarters:	1164 Ostorhegy utca 4.
Telephone:	+36 1 400-6065
E-mail:	support@gepida.com

The data you provide is stored on a server operated by the hosting provider. Only our staff or the staff operating the server have access to the data, but they are all responsible for the security of the data.

Activity description: trade in bicycles and spare parts

Purpose of processing: trade

Data processed: personal data provided by the data subject

Duration of processing and time limit for deletion of data. Data processing until the end of the website's operation or in accordance with the contractual agreement between the website operator and the hosting provider. If necessary, the data subject may request the deletion of his/her data by contacting the hosting provider.

The legal basis for processing is the consent of the data subject or processing based on law.
Data protection is based on the lawfulnes.

Rights in relation to data processing

The right to request information
You may request information from us, via the contact details provided, about what data our company processes, on what legal basis, for what purpose, from what source and for how long. Upon your request, we will send you information without delay, but within 30 days at the latest, to the e-mail address you have provided.

The right to rectification
You can ask us to correct any of your data using the contact details provided. Upon your request, we will do so without delay, but within 30 days at the latest, by sending you an e-mail to the e-mail address you have provided.

The right to erasure
You may request us to delete your data by using the contact details provided. Upon your request, we will do so without delay, but within 30 days at the latest, by sending you an e-mail to the e-mail address you have provided.

The right to blocking
You can ask us to block your data using the contact details provided. The blocking will last as long as the reason you have given us makes it necessary to store the data. Upon your request, we will do so without delay, but within 30 days at the latest, by sending you an e-mail to the e-mail address you have provided.

The right to protest
You may object to the processing of your data by using the contact details provided. We will examine the objection within the shortest possible time from the date of the request, but no later than 15 days, decide whether it is justified and inform you of our decision by e-mail.

Enforcement possibilities in relation to data processing
If you experience unlawful processing, please notify us so that we can restore the lawful status within a short period of time. We will do our utmost to resolve the problem in your interest.

If, in your opinion, the lawful status cannot be restored, please notify the authority using the following contact details:

National Authority for Data Protection and Freedom of Information
Postal address: 1374 Budapest, Pf. 603.
Address: 1055 Budapest, Falk Miksa utca 9-11.
Telephone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu
URL https://naih.hu

Laws on which the processing is based

- REGULATION (EU) No 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 Regulation (EC) No 95/46/EC (General Data Protection Regulation).

- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.

- Act LXVI of 1995 on public records, public archives and the protection of private archival material.

- Government Decree No 335/2005 (XII. 29.) on the general requirements for document management by public bodies.

- Act CVIII of 2001 on certain aspects of electronic commerce services and information society services.

- Act C of 2003 on electronic communications.

CONSENT TO THE PROCESSING OF PERSONAL DATA

Signed

NAME :
ADDRESS:
ID CARD NUMBER.:
TELEPHONE:
E-MAIL ADDRESS:

declare that by signing this document, I voluntarily AGREE to provide my personal data as indicated above to the

COMPANY NAME (DATA PROVIDER): Olimpia Kerékpár Kft.
HEADQUARTERS: 1164 BUDAPEST, Ostorhegy utca 4.
TAX NUMBER: 12216109-2-42
NAME OF REPRESANTETIVE: C. Szabó Péter

as Data Controller, for the following purposes: design, assembly and sale of bicycles.

…… ……
signature/individual signature/Olimpia Kerékpár Kft.

Date:

Information about the personal data breach to the data subject

What kind of data breach occurred	
Contact details of the Data Protection Officer / contact person	
Cause(s), consequence(s) of the data breach	
Measures to respond to the data breach	

Date: