Privacy Policy

Introduction

Kristóf Gyimóthy (Company registration number: 01-09-941423) (hereinafter: Service Provider, data controller) submits to the following prospectus.

Act CXII of 2011 on the right to information self-determination and freedom of information. Section 20 (1) of the Act stipulates that the data subject (in this case the webshop user, hereinafter: user) must be informed before the start of data processing that the data processing is based on consent or is mandatory.

Prior to the commencement of data processing, the data subject shall be clearly and in detail informed of all facts related to the processing of his / her data, in particular the purpose and legal basis of the data processing, the data controller and the duration of the data processing.

The data subject must be informed about Info tv. § 6 (1) that personal data may be processed even if obtaining the data subject's consent would be impossible or disproportionate, and the processing of personal data

necessary to fulfill a legal obligation to which the controller is subject, or
necessary for the exercise of a legitimate interest of the controller or of a third party and the exercise of that interest is proportionate to the restriction of the right to the protection of personal data.
The information should also cover the data subject's rights and remedies.

If it would be impossible or disproportionately costly to inform the persons concerned personally (as in the present case in a webshop), the information may also be provided by disclosing the following information:

a) the fact of data collection,
b) the range of stakeholders,
c) the purpose of the data collection,
d) the duration of the data processing,
e) the identity of the potential data controllers entitled to access the data,
(f) a description of the data subjects' rights and remedies in relation to the processing; and
(g) where the data processing is subject to a data protection register, the registration number of the data processing.
This data management information is based on the above content specification. The prospectus is available at http://www.oravasarlas.com/help#21

The scope of this prospectus covers data management on the Service Provider's websites (http://www.oravasarlas.com/) and subdomains.

Amendments to the prospectus will take effect upon publication at the above address. We also display the legal reference behind each chapter in the prospectus.

Interpretive concepts (§ 3)

data subject / User: any specific natural person identified or - directly or indirectly - identifiable on the basis of personal data;
personal data: data which can be contacted with the data subject, in particular the name, identification mark and knowledge of one or more physical, physiological, mental, economic, cultural or social identities of the data subject, and the inference that can be drawn from the data;
special data:
(a) personal data concerning racial origin, nationality, political opinion or party affiliation, religious or other worldview, membership of an advocacy organization, sex life,
(b) personal data concerning health status, pathological passion and criminal personal data;
consent: the voluntary and firm expression of the will of the data subject, based on adequate information and giving his or her unambiguous consent to the processing of personal data concerning him or her, in whole or in part;
protest: a statement by the data subject objecting to the processing of his or her personal data and requesting the termination of the processing or the deletion of the processed data;
"controller" means the natural or legal person, or any entity without legal personality, which alone or jointly with others determines the purpose for which the data are processed, makes and implements decisions on data processing (including the means used) or executes them with a data controller;
data management: any operation or set of operations on data, irrespective of the procedure used, in particular their collection, recording, recording, systematisation, storage, alteration, use, interrogation, transmission, disclosure, coordination or aggregation, blocking, erasure and destruction; and to prevent further use of the data, to take photographs, sound or images and to record physical characteristics capable of identifying the person (eg fingerprint or palm print, DNA sample, iris image);
data transfer: making the data available to a specific third party;
disclosure: making data available to anyone;
data erasure: making data unrecognizable in such a way that it is no longer possible to recover it;
data marking: the identification of the data in order to distinguish it;
data blocking: the identification of data for the purpose of limiting their further processing definitively or for a specified period;
data destruction: complete physical destruction of the data carrier;
data processing: the performance of technical tasks related to data management operations, regardless of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data;
data processor: a natural or legal person or an organization without legal personality who, on the basis of a contract concluded with the data controller, including the conclusion of a contract on the basis of a provision of law, processes data;
data controller: the body performing a public task which has produced data of public interest to be published compulsorily by electronic means or in the course of the operation of which this data has been generated;
informant: a body performing a public task which, if the data controller does not publish the data itself, publishes the data provided to it by the data controller on a website;
data set: the totality of the data managed in one register;
"third party" means any natural or legal person, or any entity without legal personality, other than the data subject, the controller or the processor;

Legal basis for data management (5-6§)

Personal data can be processed if
the data subject consents thereto, or
it is ordered by law or - on the basis of the authorization of law, within the scope specified therein - by a decree of a local government for a purpose based on the public interest.
Personal data may be processed even if it would be impossible or disproportionate to obtain the data subject's consent and the processing of personal data
(a) necessary to fulfill a legal obligation to which the controller is subject, or

(b) necessary for the protection of a legitimate interest of the controller or of a third party and the exercise of that interest is proportionate to the restriction of the right to the protection of personal data.
If the data subject is unable to give his or her consent due to incapacity or for other unavoidable reasons, the personal data of the data subject during the period of impediment to the protection of his or her own or another person's manageable.
The consent or subsequent approval of the legal representative of a minor who has reached the age of 16 shall not be required for the validity of his / her legal declaration containing the consent of the person concerned.
If the purpose of consent-based data processing is to perform a written contract with the data controller, the contract must contain all the information that the data subject must know, in particular the definition of the data to be processed, the duration of the data processing, the purpose of use, the transfer , recipients, the fact of using a data processor. The contract must state unequivocally that, by signing, the data subject consents to the processing of his or her data as specified in the contract.
If the personal data was collected with the consent of the data subject, the data controller shall, unless otherwise provided by law,
in order to fulfill a legal obligation incumbent on it, or
for the purpose of enforcing the legitimate interest of the controller or a third party, if the exercise of such interest is proportionate to the restriction of the right to the protection of personal data

Purposefulness of data management (§ 4 [1] - [2])

Personal data may only be processed for a specific purpose, in order to exercise a right and fulfill an obligation. At all stages of data management, the purpose of data management must be appropriate, and the collection and handling of data must be fair and lawful.
Only personal data that is necessary for the realization of the purpose of data processing and suitable for the achievement of the purpose may be processed. Personal data may only be processed to the extent and for the time necessary to achieve the purpose.

Other principles of data management (§ 4 [3] - [4])

Personal data retains this quality during data processing as long as its connection with the data subject can be restored. The connection with the data subject can be restored if the data controller has the technical conditions necessary for the restoration.

The processing shall ensure the accuracy, completeness and, where necessary, the up-to-dateness of the data, and that the data subject can only be identified for the time necessary for the purpose of the processing.

Other principles of data management (§ 4 [3] - [4])

Personal data retains this quality during data processing as long as its connection with the data subject can be restored. The connection with the data subject can be restored if the data controller has the technical conditions necessary for the restoration.

The processing shall ensure the accuracy, completeness and, where necessary, the up-to-dateness of the data, and that the data subject can only be identified for the time necessary for the purpose of the processing.

Functional data management

Act CXII of 2011 on the right to information self-determination and freedom of information. Pursuant to Section 20 (1) of the Act, the following shall be determined within the scope of the functionality of the webshop website:
a) the fact of data collection,
b) the range of stakeholders,
c) the purpose of the data collection,
d) the duration of the data processing,
e) the identity of the potential data controllers entitled to access the data,
(f) a description of the data subjects' rights in relation to data processing.
The fact of data collection, the scope of the managed data: Password, surname and first name, company name, e-mail address, telephone number, billing address, delivery address, contact name, date of registration, IP address at the time of registration.
Stakeholders: All stakeholders registered on the webshop website.
Purpose of data collection: Service provider to make full use of the website, e.g. manages the personal data of the Users for the purpose of creating a contract for the provision of the service, defining its content, modifying it, monitoring its fulfillment, invoicing the fees arising therefrom and enforcing the related claims, as well as sending newsletters.
Duration of data management, deadline for deleting data: By deleting the registration immediately. Except in the case of accounting documents, as these data must be kept for 8 years pursuant to Section 169 (2) of Act C of 2000 on Accounting.
Identity of potential data controllers entitled to access the data: Personal data may be processed by the data controller's staff, respecting the above principles.
Description of data subjects' rights related to data management: The following data can be changed on the websites: Password, surname and first name, company name, e-mail address, telephone number, billing address, delivery address, contact name. The deletion or modification of personal data can be initiated by the data subject in the following ways:
- by post at 4895 Soroksári út, 1095 Budapest,

- by e-mail to info@marketmaker.hu.

14. Legal basis of data management: the User's consent, Infotv. § 5 (1), and Act CVIII of 2001 on certain issues of electronic commerce services and information society services. Act (hereinafter: Elker Act) 13 / A. § (3).

Our principles for functional data management (Elker Act 13 / A.)

For the purpose of invoicing the fees arising from the contract for the provision of the information society service, the service provider may manage the natural personal data, address and data on the time, duration and place of the use of the information society service.
The service provider may process personal data that is technically necessary for the provision of the service in order to provide the service. If the other conditions are the same, the service provider must choose and in all cases operate the means used in the provision of the information society service in such a way that personal data is processed only if it is necessary for the provision of the service and other purposes specified in the Elker Act. necessary, but in this case only to the extent and for the time necessary.
The service provider may process data related to the use of the service for any other purpose, in particular to increase the efficiency of its service, to deliver electronic advertising or other targeted content to the user, for market research only with the prior purpose of the data processing and with the user's consent.
The user must be able to prohibit data processing before and during the use of the information society service.
The processed data must be deleted after the non-conclusion of the contract, the termination of the contract and the invoicing. The data must be deleted if the purpose of data management has ceased or if the user so provides. Unless otherwise provided by law, the deletion of data must be carried out immediately.
The service provider must ensure that the user can find out which data management purposes the service provider handles for which data management purposes, including the handling of data that cannot be directly contacted by the user, at any time before and during the use of the information society service.

Data transmission

Act CXII of 2011 on the right to information self-determination and freedom of information. Pursuant to Section 20 (1) of the Act, the following shall be determined within the scope of the webshop's data transmission activities:

the fact of data collection,
the range of stakeholders,
the purpose of the data collection,
the duration of the data management,
the identity of the potential data controllers entitled to access the data,
a description of the data subjects' rights in relation to data processing.
The fact of data management, the scope of data managed.

The scope of the transmitted data in order to carry out the delivery: Name, delivery address, telephone number, product name, amount to be paid.

The scope of the transmitted data for online payment and invoicing: Name, billing address, transaction amount, transaction title.

Stakeholders: All stakeholders involved in home delivery / online shopping.
The purpose of data management: Home delivery of the ordered product / online shopping.
Description of the data subjects' rights in relation to data processing: The data subject may request the data controller of the home delivery / online payment service provider to delete his personal data as soon as possible.
The legal basis of the data transfer: the User's consent, the Infotv. § 5 (1), and Act CVIII of 2001 on certain issues of electronic commerce services and information society services. Act 13 / A. § (3).
Identity of potential data controllers entitled to access the data: Personal data may be processed by the following, respecting the above principles:

Billingo Technologies Private Limited Company
Purpose of data management: Creating an invoice for the customer - transmitting invoice data to NAV
Headquarters: 1133 Budapest, Árbóc utca 6. 3rd floor.
Company registration number: 01-10-140802
Tax number: 27926309-2-41
Data management statement: https://www.billingo.hu/adatkezelesi-tajekoztato

Barion Payment Zrt.
Purpose of data management: to make an online payment
Address: 1117 Budapest, Infopark sétány 1. I. building 5. floor 5
Privacy statement: https://www.barion.com/hu/adatvedelmi-tajekoztato/

Webshippy Hungary Limited Liability Company

Purpose of data management: provision of warehousing, packaging and other logistics services, transmission of address data to the courier service
Address: 1044 Budapest, Ezred u. 2. B. intact. 13.
Tax number: 25569421-2-41
Privacy statement: https://webshippy.com/adatkezelesi-tajekoztato/

GLS General Logistics Systems Hungary Kft.

Purpose of data management: delivery of packages, notification of customers about the status of delivery
Address: 2351 Alsónémedi, GLS Európa utca 2.
Privacy statement: https://gls-group.eu/EN/en/adata-assembly-tajection
UNAS Online Kft.

Purpose of data management: Operation of a webshop engine, during which all the data provided by the customer on the website are accessed
Address: H-9400 Sopron, Kőszegi út 14.
Data management statement: https://unas.hu/adatkezelesi-tajekoztato

Data security (§ 7)

The controller is obliged to plan and carry out data management operations in such a way as to ensure the protection of the privacy of data subjects.
Within the scope of the data controller or activity, the data processor is obliged to ensure the security of the data, is also obliged to take the technical and organizational measures and to establish the procedural rules necessary for the enforcement of the Info Act and other data and confidentiality rules.
The data shall be protected by appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, accidental destruction and damage, and loss of access due to changes in the technology used.
In order to protect the data files processed electronically in the various registers, an appropriate technical solution must be used to ensure that the data stored in the registers cannot be linked directly to one of the data subjects, unless permitted by law.
During the automated processing of personal data, the data controller and the data processor shall provide additional measures
prevent unauthorized data entry;
prevent the use of automatic data-processing systems by unauthorized persons using data communication equipment;
the verifiability and traceability of the bodies to which personal data have been or may be transmitted using data communication equipment;
the controllability and traceability of which personal data have been input into automated data-processing systems, when and by whom;
the resilience of installed systems in the event of a breakdown; and
that errors in automated processing be reported.
The controller and the processor must take into account the state of the art when defining and applying data security measures. Of the several possible data management solutions, the one that provides a higher level of protection of personal data should be chosen, unless this would impose a disproportionate burden on the controller.

Remedies

User may object to the processing of his / her personal data if
a) the processing or transmission of personal data is necessary only for the fulfillment of a legal obligation to the Service Provider or for the enforcement of the legitimate interest of the Service Provider, the data recipient or a third party, unless the data processing is

ordered by law;
(b) personal data are used or transmitted for the purposes of direct business acquisition, public opinion polling or scientific research;
c) in other cases specified by law.
The Service Provider shall examine the protest within the shortest time from the submission of the application, but not later than within 15 days, make a decision on the merits of the application and inform the applicant of its decision in writing. If the Service Provider establishes the validity of the data subject's protest, it terminates the data processing, including further data collection and data transfer, and blocks the data, and notifies all those to whom it has previously transmitted the data subject concerned of the protest, and who are obliged to take action to enforce the right to protest.
If the User does not agree with the decision made by the Service Provider, he may appeal against it to the court within 30 days of its notification. The court is acting out of turn.
Complaints against possible breaches of the data controller can be lodged with the National Data Protection and Freedom of Information Authority:
National Data Protection and Freedom of Information Authority

1125 Budapest, Szilágyi Erzsébet avenue 22 / C.

Mailing address: 1530 Budapest, Mailbox: 5.

Phone: +36 -1-391-1400

Fax: + 36-1-391-1410

E-mail: ugyfelszolgalat@naih.hu

Rights of data subjects (§ 14-19)

The data subject may request the Service Provider to provide information on the handling of his / her personal data, request the correction of his / her personal data, and request the deletion or blocking of his / her personal data, with the exception of mandatory data processing. The User may request the above in an e-mail addressed to the Operator, which must be sent to the e-mail address info@marketmaker.hu.
At the request of the data subject, the data controller shall provide information on the data processed by the data subject and processed by the data controller, their source, purpose, legal basis, duration, name, address and activities related to the data processing, as well as the legal basis and the recipient of the transfer.
In order to check the lawfulness of the data transfer and to inform the data subject, the data controller shall keep a data transfer register containing the date of transfer of personal data processed by him, the legal basis and recipient of the transfer, the definition of the transferred personal data and other data specified by law.
The data controller shall provide the information in writing in a comprehensible form at the request of the data subject as soon as possible after the submission of the request, but no later than within 30 days. The information is free.
At the request of the User, the Service Provider provides information on the data processed by it, their source, purpose, legal basis, duration, name, address and activities related to data processing of any data processor, and - in case of transfer of personal data of the data subject - legal basis and recipient. The Service Provider shall provide the information in writing, in a comprehensible form, as soon as possible after the submission of the application, but not later than within 30 days. The information is free.
The Service Provider shall correct the personal data if the personal data does not correspond to reality and the personal data corresponding to reality is available to the data controller.
Instead of deleting, the Service Provider blocks the personal data if the User so requests or if, on the basis of the information available to him, it can be assumed that the deletion would harm the legitimate interests of the User. Blocked personal data may only be processed for as long as the purpose of the data processing, which precluded the deletion of personal data, exists.
The Service Provider deletes the personal data if its processing is illegal, the User requests, the processed data is incomplete or incorrect - and this condition cannot be legally remedied - provided the deletion is not excluded by law, the purpose of data processing is terminated or the data storage expired, it was ordered by a court or the National Data Protection and Freedom of Information Authority.
The controller shall flag the personal data processed by him or her if the data subject disputes their correctness or accuracy, but the inaccuracy or inaccuracy of the disputed personal data cannot be clearly established.
The rectification, blocking, marking and erasure shall be notified to the data subject and to all persons to whom the data have previously been transmitted for data processing purposes. The notification may be omitted if it does not harm the legitimate interests of the data subject in view of the purpose of the processing.
If the controller does not comply with the request for rectification, blocking or erasure of the data subject, he shall state in writing the reasons in fact and in law for rejecting the request for rectification, blocking or erasure within 30 days of receipt of the request. If the request for rectification, erasure or blocking is rejected, the controller shall inform the data subject of the possibility of legal redress and recourse to the Authority.

Judicial enforcement (§ 22)

The data controller is obliged to prove that the data processing complies with the provisions of the law. The recipient of the data must prove the lawfulness of the data transfer.
The trial falls within the jurisdiction of the tribunal. The action may, at the option of the person concerned, also be brought before the court of the place where he or she resides or stays.
A party who does not otherwise have legal capacity to sue may also be a party to a lawsuit. The Authority may intervene in the proceedings in order for the person concerned to succeed.
If the court grants the request, it obliges the data controller to provide the information, to correct, block, delete the data, to annul the decision made by automated data processing, to respect the data subject's right of objection or to release the data requested by the data recipient.
If the court rejects the data recipient's request, the data controller is obliged to delete the personal data of the data subject within 3 days from the notification of the judgment. The data controller is obliged to delete the data even if the data recipient does not go to court within the specified time limit.
The court may order the publication of its judgment, by publishing the identity of the controller, if the interests of data protection and the protected rights of a larger number of data subjects so require.

Closing remarks

During the preparation of the prospectus, we took into account the following legislation:

- - REGULATION (EU) 2016/679 of the European Parliament and of the Council

- 2011 CXII. Act - on the right to information self-determination and freedom of information (hereinafter: Infotv.)

- CVIII of 2001 Act - on certain issues of electronic commerce services and services related to the information society (mainly Section 13 / A)

- XLVII of 2008 Act on the Prohibition of Unfair Commercial Practices against Consumers;

- XLVIII of 2008 Act - on the basic conditions and certain restrictions of commercial advertising (especially § 6)

- 2005 XC. Electronic Freedom of Information Act
- Act C of 2003 on electronic communications (specifically Section 155)
- 16/2011. s. Opinion on the EASA / IAB Recommendation on Best Practices for Behavioral Online Advertising

Kristóf Gyimóthy does not take any financial or legal responsibility for any prescriptions or inaccurate prices.