

Last update date: 2024.01.10

RETROSC.HU PRIVACY POLICY

RETR-O-SC

Introduction

RETR-O-SC (1188 Budapest - XVIII. district, Póth Irén u. 87/a/2., tax number: 18256172-1-43, company registration number: 11711) (hereinafter referred to as the "Service Provider", "Data Controller") is subject to the following policy:

Pursuant to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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), the following information is provided.

This Privacy Policy governs the processing of data on the following websites/mobile applications:
<https://www.retrosc.hu/>

The Privacy Policy is available at: <https://www.retrosc.hu//adatvedelem>

Amendments to this policy will enter into force upon publication at the above address.

The controller and contact details

Name: RETR-O-SC

Address: 1188 Budapest - XVIII. district, Póth Irén u. 87/a/2.

E-mail: info@retrosc.hu

Phone: none

No. of telephone No. of address

"personal data" means 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;

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

"controller" means a 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 designation of the controller may also be determined by Union or Member State law;

'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a controller;

'recipient' means a natural or legal person, public authority, agency or any other body to whom or with which personal data are disclosed, whether or not a third party. 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;

'consent of the data subject' means 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 relating to him or her;

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

Principles governing the processing of personal data

Personal data:

must be lawful, fair and transparent for the data subject ("lawfulness, fairness and transparency");

collected only for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes shall not be considered incompatible with the original purposes in accordance with Article 89(1) ('purpose limitation');

the processing must be adequate, relevant and limited to what is necessary for the purposes for which it is intended ('data minimisation');

be accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data which are inaccurate for the purposes for which they are processed are erased or rectified without undue delay ('accuracy');

it must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be kept for longer periods only if the personal data will be processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to the implementation of appropriate technical and organisational measures as provided for in this Regulation to safeguard the rights and freedoms of data subjects ('limited storage');

processing must be carried out in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage ('integrity and confidentiality'), by implementing appropriate technical or organisational measures.

The controller is responsible for compliance with the above and must be able to demonstrate such compliance ("accountability").

The controller declares that its processing will be carried out in accordance with the principles set out in this point.

Processing in relation to the use of a sale/service

Personal data	Purpose of processing	Legal basis
Surname and first name	Necessary for contacting you, making a purchase, issuing a correct invoice.	Article 6(1)(b) GDPR and § 13/A(3) Elker Act.
E-mail address	Contact.	Article 6 (1) (b) GDPR and § 13/A (3) Elker tv.
Phone number	Contact, more efficient coordination of billing issues.	Article 6(1)(b) GDPR and Section 13/A(3) Elker tv.
Billing name and address	The issuing of proper invoices, as well as the creation, definition of the content, modification and monitoring of the performance of the contract, the invoicing of the fees arising from it and the enforcement of claims related to it.	Article 6(1)(c) and Article 169(2) of Act C of 2000 on accounting
Date of order/purchase	Execution of a technical operation.	Article 6(1)(b) GDPR and Section 13/A(3) Elker Act.
IP address of the order/purchase	Execution of a technical operation.	Article 6 (1) (b) GDPR and § 13/A (3) Elker tv.

2. Data subjects: all data subjects who shop on the website.

3. The controller shall inform the data subject of the erasure of any personal data provided by the data subject by electronic means pursuant to Article 19 of the GDPR. If the data subject's request for erasure also includes the e-mail address provided by him or her, the controller shall erase the e-mail address following the notification. Except in the case of accounting records, since pursuant to Article 169 (2) of Act C of 2000 on Accounting, these data must be kept for 8 years. The contractual data of the data subject may be deleted after the expiry of the civil law limitation period on the basis of a request for deletion by the data subject.

The accounting documents (including general ledger accounts, analytical or detailed records) directly and indirectly supporting the accounting accounts must be kept for at least 8 years in a legible form, retrievable by reference to the accounting records.

The data subject may request the controller to access, rectify, erase or restrict the processing of personal data concerning him or her, and

the data subject has the right to data portability and the right to withdraw consent at any time.

by post at the address Póth Irén u. 87/a/2., 1188 Budapest - XVIII. district, 1188 Budapest - XVIII. district,

7. Legal basis for processing:

Article 6 (1) (b) and (c) of the GDPR,

Article 6.6(b)(1)(b)(c) of GDPR, Section 6.1.1.1, Paragraph 2:

The service provider may process personal data which are technically indispensable for the provision of the service. The service provider must, other conditions being equal, choose and in any case operate the means used in the provision of the information society service in such a way that personal data are processed only if absolutely necessary for the provision of the service and for the fulfilment of the other purposes specified in this Act, but in this case only to the extent and for the duration necessary.

3. in the case of invoicing in accordance with accounting legislation, Article 6(1)(c).

4. in the case of enforcement of claims arising from the contract, 5 years pursuant to § 6:21 of Act V of 2013 on the Civil Code.

§ 6:22 [Limitation period]

(1) Unless otherwise provided by this Act, claims shall be time-barred after five years.

(2) The limitation period shall begin to run when the claim becomes due.

(3) An agreement to change the limitation period shall be in writing.

(4) An agreement excluding the limitation period is void.

the processing is necessary for the performance of a contract.

You are obliged to provide the personal data in order for us to fulfil your order.v

Failure to provide the data will result in our inability to process your order.

Processing of cookies (cookie)

Purpose of processing: identification of users, tracking of visitors, personalisation of the operation.

Type of cocy	Legal basis for processing	Duration of processing
Session cookies or other cookies that are essential for the functioning of the website	Article 6(1)(f) GDPR. Legitimate interest of the controller for the purpose of operating the website, ensuring the functionality and essential functions of the website and the security of the computer system.	The relevant the relevant visitor session period
Persistent or saved cookies	Article 6(1)(f) GDPR. Legitimate interest of the controller for the purposes of operating the website, ensuring the functionality and essential functions of the website and	Data processing lasts until the data subject deletes the cookie or cookies with a precise expiry date (persistent, saved) are stored on the computer until they are deleted, but at the

	the security of the computer system	latest until their expiry date
Statistical, marketing cookies	Article 6(1)(a) GDPR	1 month - 2 years

6. Identity of the potential controllers who have access to the data: personal data may be accessed by the controller.

7. Description of data subjects' rights in relation to data processing.

8. Most browsers used by our users allow you to set which cookies should be saved and allow you to delete (certain) cookies again. If you restrict the saving of cookies on specific websites or do not allow third party cookies, this may in certain circumstances lead to our website no longer being fully usable. Here you will find information on how to customise your cookie settings for standard browsers:

Google Chrome (<https://support.google.com/chrome/answer/95647?hl=hu>)

Internet Explorer (<https://support.microsoft.com/hu-hu/help/17442/windows-internet-explorer-delete-manage-cookies>)

Firefox (<https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn>)

Safari (<https://support.apple.com/hu-hu/guide/safari/sfri11471/mac>)

Use Google Ads conversion tracking

The online advertising program "Google Ads" is used by the data controller and within its framework, the Google conversion tracking service is used. Google Conversion Tracking is an analytics service provided by Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; "Google").

When you access a website through a Google ad, a cookie is placed on your computer for conversion tracking. These cookies have a limited validity and do not contain any personal data, so the User cannot be identified by them.

When the User browses certain pages of the website and the cookie has not expired, Google and the data controller can see that the User has clicked on the ad.

Each Google Ads customer receives a different cookie, so they cannot be tracked through the Ads customers' websites.

The information obtained through conversion tracking cookies is used to provide conversion statistics for Ads customers who opt for conversion tracking. Customers are then informed of the number of users who click on their ad and are referred to a page with a conversion tracking tag. However, they do not have access to information that would allow them to identify any user.

If you do not wish to participate in conversion tracking, you can opt out by disabling the option to set cookies in your browser. You will then not be included in the conversion tracking statistics.

For more information and to read Google's privacy statement, please visit <https://policies.google.com/privacy>

Google Analytics

This website uses Google Analytics, a web analytics service provided by Google Inc ("Google"). Google Analytics uses "cookies", text files that are stored on your computer to help the website analyze how users use the website you have visited.

The information generated by the cookie about the website you use is usually transmitted to and stored by Google on servers in the United States. By activating the IP anonymisation on the website, Google will previously shorten the User's IP address within the Member States of the European Union or in other states party to the Agreement on the European Economic Area.

Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and shortened there. On behalf of the operator of this website, Google will use this information to evaluate your use of the website, to compile reports on website activity for the website operator and to provide other services relating to website activity and internet usage.

Google Analytics will not associate the IP address transmitted by the User's browser with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of this website. You may also prevent Google from collecting and processing information about your use of the website (including your IP address) by means of cookies by downloading and installing the browser plug-in available at <https://tools.google.com/dlpage/gaoptout?hl=hu>

Newsletter, DM activity

3. In this case, the Service Provider shall delete all personal data necessary for sending advertising messages from its records and shall not contact the User with further advertising offers. The User may unsubscribe from advertising by clicking on the link in the message.

Personal data	Purpose of processing	Legal basis
Name, e-mail address.	Identification, to enable subscription to the newsletter/special offers.	Consent of the data subject, Article 6(1)(a). Article 6(5) of Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions on Commercial Advertising Activities.
Date of subscription	Performing a technical operation.	Consent of the data subject, Article 6(1)(a). Article 6(5) of Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions on Commercial Advertising Activities.
IP address at the time of subscription	operation. Execution of a technical	Consent of the data subject, Article 6(1)(a). Article 6(5) of Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions on Commercial Advertising Activities.

5. Data subjects: all data subjects who subscribe to the newsletter.

Purpose of data processing.

The data subject may request from the controller access to, rectification, erasure or restriction of processing of personal data concerning him or her, and

object to the processing of his or her personal data; and

the right to data portability and the right to withdraw consent at any time.

by post at the address Póth Irén u. 87/a/2., 1188 Budapest - XVIII. district, 1188 Budapest - XVIII. district,

by e-mail to the e-mail address info@retrosc.hu,

by telephone at the number no.

11. The data subject may unsubscribe from the newsletter at any time, free of charge.

12.

The processing of the data is based on your consent and the legitimate interest of the service provider.

You are obliged to provide personal data if you wish to receive newsletters from us.

Failure to provide this information will result in our inability to send you a newsletter.

please note that you can withdraw your consent at any time by clicking on the unsubscribe button.

the withdrawal of consent does not affect the lawfulness of the processing based on consent prior to its withdrawal.

Complaints handling

Personal data	Purpose of processing	Legal basis
Surname and first name	Identification, contact details.	Article 6(1)(c) and Article 17/A(7) of Act CLV of 1997 on Consumer Protection.
E-mail address	Contact details.	Article 6(1)(c) and Article 17/A(7) of Act CLV of 1997 on Consumer Protection.
Telephone number	Contact.	Article 6(1)(c) and Article 17/A(7) of Act CLV of 1997 on Consumer Protection.
Billing name and address	Identification, handling of quality complaints, questions and problems related to the products/services ordered.	Article 6(1)(c) and Article 17/A(7) of Act CLV of 1997 on Consumer Protection.

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

the data subject has the right to data portability and the right to withdraw consent at any time

6. The data subject may request access to, erasure, rectification or restriction of processing of personal data and portability of the data in the following ways:

by post to the address Póth Irén u. 87/a/2., 1188 Budapest - XVIII. district, 1188 Budapest - XVIII. district,

by e-mail to the e-mail address info@retrosc.hu,

by telephone at the number no.

7.

The provision of personal data is based on a legal obligation.

The processing of personal data is a precondition for the conclusion of the contract.

You are obliged to provide the personal data in order to allow us to deal with your complaint.

failure to provide the data will result in our inability to handle your complaint.

Recipients to whom personal data are disclosed

"recipient" means a natural or legal person, public authority, agency or any other body with whom or to which personal data is disclosed, whether or not a third party.

1. Processors (those who carry out processing on behalf of the controller)

The controller uses processors to facilitate its own processing activities and to fulfil its contractual and legal obligations with data subjects.

The controller shall place great emphasis on using only processors that offer adequate guarantees to implement appropriate technical and organisational measures to ensure compliance with the requirements of the GDPR and to protect the rights of data subjects.

The processor and any person acting under the control of the controller or the processor who has access to the personal data shall process the personal data covered by this Policy only in accordance with the instructions of the controller.

The controller shall be legally responsible for the activities of the processor. A processor shall be liable for damage caused by processing only if it has failed to comply with the obligations specifically imposed on processors by the GDPR or if it has disregarded or acted contrary to lawful instructions from the controller.

The processor has no substantive decision-making power with regard to the processing of the data.

The data controller may use a hosting service provider to provide the IT background and a courier service as a data processor for the delivery of ordered products.

2. Certain data processors

Data processing activities	Name, address, contact details
Hosting service	Company name: Rackhost Zrt. Registered office. E-mail address: info@nextserver.hu Phone: +36 1 445 1300 Fax: +36 1 700 1650 Tax number: 25333572-2-06 Company registration number: 06-10-000489 Account holder bank: CIB Bank Számlasszám: 10700433-67330115-51100005
Other data processor (e.g. online invoicing, web development, marketing)	MailChimp The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA privacy@mailchimp.com

"third party" means 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.

3. Transfers of data to third parties

Third party data controllers process the personal data we disclose to them on their own behalf and in accordance with their own privacy policies.

Activities of the data controller	Name, address, contact details
Transport	-
Online payment	-

Social networking sites

Fact of data collection, scope of data processed: name registered on social networking sites Meta/Twitter/Pinterest/Youtube/Instagram etc. and public profile picture of the user.

Data subjects.

The purpose of the data collection.

The duration of the processing, the time limit for the deletion of the data, the identity of the possible controllers of the data and the rights of the data subjects in relation to the processing of the data.

The data are processed on the social networking sites, so the duration of the processing, the way in

which the data are processed and the possibilities for deleting and modifying the data are governed by the rules of the social networking site concerned.

Legal basis for processing: the data subject's voluntary consent to the processing of his or her personal data on social networking sites.

Customer relations and other processing

If the data subject has any questions or problems when using our services, he or she may contact the data controller by the means indicated on the website (telephone, e-mail, social networking sites, etc.).

The data controller will delete the received e-mails, messages, data provided by telephone, Meta, etc., together with the name and e-mail address of the interested party and other personal data voluntarily provided by the interested party, after a maximum of 2 years from the date of the communication.

Any processing of data not listed in this notice will be notified at the time the data is collected.

In exceptional cases, the Service Provider is obliged to provide information, data or documents in response to a request from a public authority or other bodies authorised by law.

In such cases, the Service Provider shall only disclose personal data to the requesting party - provided that the latter has indicated the precise purpose and scope of the data - to the extent and to the extent that is indispensable for the purpose of the request.

Rights of the data subjects

1. Right of access

You have the right to receive feedback from the controller as to whether or not your personal data are being processed and, if such processing is taking place, the right to access your personal data and the information listed in the Regulation.

2. Right to rectification

You have the right to have inaccurate personal data relating to you corrected by the controller without undue delay upon your request. Taking into account the purposes of the processing, you have the right to request the rectification of incomplete personal data, including by means of a supplementary declaration.

3. Right to erasure

You have the right to obtain from the controller the erasure of personal data relating to you without undue delay upon your request, and the controller is obliged to erase personal data relating to you without undue delay under certain conditions.

4. Right to be forgotten

If the controller has disclosed the personal data and is under an obligation to erase it, the controller will take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform the controllers that have processed the data that you have requested the erasure of the links to or copies of the personal data in question.

5. Right to restriction of processing

You have the right to obtain, at your request, the restriction of processing by the controller if one of the following conditions is met:

You contest the accuracy of the personal data, in which case the restriction shall apply for a period of time which allows the controller to verify the accuracy of the personal data;

the processing is unlawful and you oppose the erasure of the data and instead request the restriction of their use;

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

you have objected to the processing; in this case, the restriction applies for a period of time until it is established whether the controller's legitimate grounds override your legitimate grounds.

6. Right to data portability

You have the right to receive the personal data concerning you that you have provided to a controller in a structured, commonly used, machine-readable format and the right to transmit these data to another controller without hindrance from the controller to whom you have provided the personal data.

7. Right to object

In the case of processing based on legitimate interest or public authority as legal grounds, you have the right to object at any time, on grounds relating to your particular situation, to the processing of your personal data, including profiling based on the aforementioned provisions.

8. Objection in case of direct marketing

Where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of personal data concerning you for such purposes, including profiling, where it is related to direct marketing. If you object to the processing of your personal data for direct marketing purposes, your personal data may no longer be processed for those purposes.

9. Automated decision-making in individual cases, including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

The previous paragraph does not apply where the decision:

necessary for the conclusion or performance of a contract between you and the controller;

it is permitted by Union or Member State law applicable to the controller which also lays down appropriate measures to protect your rights and freedoms and legitimate interests; or

is based on your explicit consent.

Time limit for taking action

The controller shall inform you of the action taken on the above requests without undue delay and in any event within 1 month of receipt of the request.

If necessary, this may be extended by 2 months. The controller shall inform you of the extension, stating the reasons for the delay, within 1 month of receipt of the request.

If the controller does not take action on your request, it shall inform you without delay and at the latest within one month of receipt of the request of the reasons for non-action and of your right to lodge a complaint with a supervisory authority and to seek judicial remedy.

Security of processing

The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the scale of the risk, taking into account the state of the art and the cost of implementation, the nature, scope, context and purposes of the processing, and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons, including, where appropriate:

pseudonymisation and encryption of personal data;

ensuring the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data;

in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner;

a procedure for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures taken to ensure the security of data processing.

The data processed must be stored in such a way as to prevent unauthorised access. By establishing physical storage and filing arrangements for paper-based data media and by using a centralised access management system for data in electronic format.

The method of storing the data by computerised means should be such that they can be deleted at the end of the deletion period, taking into account any different deletion deadline, or when otherwise necessary. Erasure shall be irreversible.

Paper-based data media should be deprived of personal data by means of shredding or by using an external organisation specialised in shredding. In the case of electronic data media, physical destruction and, where necessary, prior secure and irretrievable deletion of the data shall be ensured in accordance with the rules on the disposal of electronic data media.

The controller shall take the following specific data security measures:

In order to ensure the security of personal data processed on paper, the Service Provider applies the following measures (physical protection):

Store documents in a secure, lockable dry room.

Where personal data processed on paper are digitised, the rules applicable to digitally stored documents shall apply

The Service Provider's data controller may only leave the premises where data processing is taking place in the course of his work by locking the data media entrusted to him or by locking the room in question.

Personal data may only be accessed by authorised persons and may not be disclosed to third parties.

The Service Provider's building and premises are equipped with fire and property protection equipment.

IT protection

Computers and mobile devices (other data carriers) used in the course of data processing are the property of the Service Provider.

The computer system containing personal data used by the Service Provider is protected against viruses.

To ensure the security of digitally stored data, the Service Provider uses data backups and archiving.

Access to the central server computer is only permitted to duly authorised and designated persons.

Access to the data on the computers is only possible with a user name and password.

Informing the data subject of the data breach

If the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall inform the data subject without undue delay.

The information given to the data subject shall clearly and prominently describe the nature of the personal data breach and provide the name and contact details of the data protection officer or other contact person who can provide further information; describe the likely consequences of the personal data breach; describe the measures taken or envisaged by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

The data subject need not be informed if any of the following conditions are met:

the controller has implemented appropriate technical and organisational protection measures and those measures have been applied in relation to the data affected by the personal data breach, in particular measures, such as the use of encryption, which render the data unintelligible to persons not authorised to access the personal data;

the controller has taken additional measures following the personal data breach to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

the provision of information would require a disproportionate effort. In such cases, the data subjects shall be informed by means of publicly disclosed information or by means of a similar measure which ensures that the data subjects are informed in an equally effective manner.

Where the controller has not yet notified the data subject of the personal data breach, the supervisory authority may, after having considered whether the personal data breach is likely to present a high risk, order the data subject to be informed.

Notification of a personal data breach to the authority

The controller shall notify a personal data breach to the supervisory authority competent under Article 55 without undue delay and, where possible, no later than 72 hours after the personal data breach has come to its attention, unless the personal data breach is unlikely to present a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, it shall be accompanied by the reasons justifying the delay.

Review in case of mandatory processing

Unless the duration of the mandatory processing or the periodic review of its necessity is specified by law, by a regulation of a local authority or by a legally binding act of the European Union, the controller shall review, at least every three years from the start of the processing, whether the

processing of personal data processed by the controller or by a processor acting on its behalf or under its instructions is necessary for the purposes of the processing.

The controller shall document the circumstances and the results of this review, keep this documentation for ten years after the review and make it available to the National Authority for Data Protection and Freedom of Information (hereinafter referred to as the Authority) upon request.

Possibility to lodge a complaint

A complaint against a possible infringement by the controller may be lodged with the National Authority for Data Protection and Freedom of Information:

National Authority for Data Protection and Freedom of Information

1055 Budapest, Falk Miksa utca 9-11.

Address for correspondence: 1363 Budapest, Pf. 9.

Phone: +36 -1-391-1400

Fax: +36-1-391-1410

E-mail: ugyfelszolgalat@naih.hu

Closing address

The following legislation has been taken into account in the preparation of this prospectus:

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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 (hereinafter referred to as the "Infotv.");

Act CVIII of 2001 - on certain aspects of electronic commerce services and information society services (in particular Article 13/A);

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

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

Act XC of 2005 on Freedom of Electronic Information;

Act C of 2003 on Electronic Communications (specifically § 155);

Opinion No 16/2011 on the EASA/IA Recommendation on best practice in behavioural online advertising;

Recommendation of the National Authority for Data Protection and Freedom of Information on data protection requirements for prior information.

Retrosc.hu Privacy Policy (Date of entry into force: 19.01.2024)

Date of last update: 10.01.2024.01.2024