

Kristinus.hu

Privacy Policy

In brief

Personal data shall be collected and controlled only in compliance with laws.

DM mails shall be sent only if they are specifically consented to by the data subject. System messages can be sent without consent.

Data shall be stored under the most secure possible conditions.

Disclosure of personal data to third party is subject to consent.

Any data subject shall be informed of his stored personal data and the data subject may also request for the deletion of his personal data on our contact details at any time.

Introduction

KRISTINUS BORBIRTOK Korlátolt Felelősségű Társaság (8713 Kéthely, Hunyadi utca 99., corporate registration number: 14 09 308142, tax number: 14321694-2-14), (hereinafter: Service Provider, Controller) undertakes to be bound by the following policy.

Data handling registration number: NAIH-100973/2016.

Section 20 (1) of act CXII of 2011 on informational self-determination and freedom of information states that prior to control being initiated the data subject (in this case the person using the website: the user) must be informed of whether the control is to be conducted **on the grounds of consent** or is mandatory.

Prior to control being initiated the data subject must be explicitly informed in details of every fact relating to the control of his data, and therefore in particular, of the **objective of the control and its legal grounds, the individual authorised to control and process the data and the duration of the control process**.

Under section 6 (1) of the Information Act the data subject shall also be informed that the personal data may also be controlled if it is not possible to obtain the consent of the data subject or even if the cost of doing so is excessively high and the personal data

- must be controlled to fulfil legal obligations applicable to the controller, or
- must be controlled to enforce the rightful interests of the controller or third parties and the enforcement of such interests is proportionate to the restrictions pertaining to the right to the protection of personal data.

Such information must equally detail the rights and legal redress opportunities the data subject has in connection with the data control.

Should it be impossible to personally inform the data subject or the cost of this proves excessively high (such as, on a website), information may also be provided by disclosing the following information:

- a) the fact of the data collection,
- b) data subjects,
- c) the objective of the data collection,
- d) duration of the control,
- e) possible controllers authorised to obtain the personal data,
- f) providing information on the rights and legal redress opportunities in connection with the control of the data pertaining to the data subjects, and
- g) control registration number, if the control is subject to data protection registration.

This privacy policy, based on the above terms and it is to regulate the control of the following websites: <http://www.kristinus.hu> and <http://www.kristinusborbirtok.hu>. The policy is accessible from the following website: <http://www.kristinus.hu/adatvedelem>

Any amendment to this policy shall take effect upon the publication thereof on the abovementioned website.

Definitions *(Section 3)*

1. *data subject/User* shall mean any natural person identified or directly or indirectly identifiable on the basis of personal data;
2. *personal data* shall mean data relating to the data subject, in particular the name and identification number of the data subject, as well as one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject;
3. *controller* shall mean a natural or legal person, or organisation without legal personality which alone or jointly with others determines the purposes and means of the control of the data; makes and executes decisions concerning data control (including the means used) or contracts a data processor to execute it;
4. *data control* shall mean any operation or the totality of operations performed on the data, regardless of the procedure applied; in particular, data collecting, recording, registration, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing, as well as preventing the further use of the data, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as, fingerprints or palm prints, DNA samples, iris scans);
5. *data processing* shall mean undertaking technical tasks in connection with data control operations, regardless of the method and means used for executing the operations, as well as the place of use, provided that the technical task is performed on the data;
6. *data processor* shall mean natural or legal person or organisation without legal personality processing the data on the grounds of a contract concluded with the controller, including contracts conducted by right of laws;
7. *data security incident* shall mean unauthorized control or processing of personal data, in particular, unauthorised access, modification, transfer, disclosure, deletion or destruction as well as accidental destruction and damage.

Data Control related to Operating a Web Shop

1. According to section 20 (1) of act CXII of 2011 on informational self-determination and freedom of information the following terms shall be identified in relation to the data control when operating the web shop:

- a) the fact of the data collection,
- b) data subjects,
- c) the objective of the data collection,
- d) duration of the control,
- e) possible controllers authorised to obtain the data,
- f) providing information on the rights of the data subjects in connection with the control of the data.

2. Fact of the data collection, scope of the controlled data and objective of the control:

Personal data	Objective of the data control
Password	This is for secure logging onto the user account.
Surname and given name	Required for the link, purchase and regular invoicing.
E-mail address	For communications.
Telephone number	Contact; for efficient communications concerning issues relating to invoicing and delivery.
Name and address for invoicing	For the purposes covering regular invoicing, conclusion of contract, identification and amendment of the content thereof, monitoring the performance, invoicing as well as enforcement of the claims resulting from the performance.
Name and address for delivery	For making the delivery possible.
Date of purchase/registration	Execution of technical operation.
IP address at the purchase/registration	Execution of technical operation.

E-mail addresses do not necessarily contain personal data.

- 3. Data subjects shall be all the persons registering/making purchases on the web shop site.
- 4. Duration of the data control, deadline for the deletion of the data: Immediately upon the deletion of the registration. With the exception of the accounting documents, since under section 169 (2) of act C of 2000 on accounting such data shall be retained for a minimum period of 8 years.

The accounting documents for direct or indirect support of bookkeeping records (including ledger accounts, analytical records and registers) shall be retained for minimum period of 8 years, shall be readable and accessible by code of reference indicated in the bookkeeping records.

5. Possible controllers authorized to obtain personal data. Personal data may be controlled by the sales and marketing colleagues of the data controller, in compliance with the abovementioned principles.
6. Providing information on the rights of the data subjects in connection with the control of the data: The data subject may initiate the deletion or modification of his personal data by the following means:
 - via the post: at the address 8713 Kéthely, Hunyadi utca 99,
 - via e-mail: at the address info@kristinus.hu,
 - over phone: phone number +36 85 539 014.
7. Data of the processor (web hosting) hired for the data controlling:

Amazon Web Services LLC
P.O. Box 81226, Seattle
WA 98108-1226, USA

8. Control registration number: in progress..
9. Legal grounds for the data control: consent of the User, as set out in section 5 (1) of the Information Act and section 13/A (3) Act CVIII of 2001 on certain issues of electronic commerce services and information society services (hereinafter: Electronic Commerce Act):

The service provider may process personal data indispensable for providing the service for technical reasons. Should other conditions be identical, the service provider shall select and operate the means applied in the course of providing information society service at all times, so that personal data shall be processed only if it is absolutely indispensable for providing the service or achieving other objectives stipulated in this Act, and only to the required extent and duration.

Reservation of Room

1. According to section 20 (1) of act CXII of 2011 on informational self-determination and freedom of information the following terms shall be identified in relation to the reservation of room and data control:
 - a) the fact of the data collection,
 - b) data subjects,
 - c) the objective of the data collection,
 - d) duration of the control,
 - e) possible controllers authorised to obtain the data,
 - f) providing information on the rights of the data subjects in connection with the control of the data.
2. Fact of the data collection, scope of the controlled data and objective of the control:

Personal data	Objective of the data control
Surname and given name	To the contact, required to the identification.
Telephone number	Communications.
Address	Identification.
Date of the reservation	Execution of technical operation.
Reservation IP address	Execution of technical operation.

3. Data subjects: all the persons making reservation on the website.
4. Duration of the data control, deadline for the deletion of the personal data: The controller shall control the personal data until the deletion is requested by the data subject.
5. Possible controllers authorized to obtain personal data: Personal data may be controlled by the colleagues of the competent hotelier and Vinotel, in compliance with the abovementioned principles.
6. Providing information on the rights of the data subjects in connection with the control of the data: The data subject may initiate the deletion or modification of his personal data by the following means:
 - via the post: at the address 8713 Kéthely, Hunyadi utca 99,
 - via e-mail: at the address info@kristinus.hu,
 - over phone: phone number +36 85 539 014.
7. Data of the processor (web hosting and IT service provider accepting the reservation) hired for the data controlling:

Amazon Web Services LLC
 P.O. Box 81226, Seattle
 WA 98108-1226, USA

HostWare Kft.
 MT-HostWare Számítástechnikai Kft.
 1149 Budapest, Róna utca 120.
 (+36-1) 469-9000
 (+36-1) 469-9009
 hostware@hostware.hu
www.hostware.hu

8. Legal grounds for the data control: consent of the User, as set out in section 5 (1) of the Information Act and section 13/A (3) Act CVIII of 2001 on certain issues of electronic commerce services and information society services (hereinafter: Electronic Commerce Act):

The service provider may process personal data indispensable for providing the service for technical reasons. Should other conditions be identical, the service provider shall select and operate the means applied in the course of providing information society service at all times, so that personal data shall be processed only if it is absolutely indispensable for providing the service or achieving other objectives stipulated in this Act, and only to the required extent and duration.

Managing Cookies

1. According to section 20 (1) of act CXII of 2011 on informational self-determination and freedom of information the following terms must be set out
2. in respect of the data control relating to the website cookies:
 - a) the fact of the data collection,
 - b) data subjects,
 - c) the objective of the data collection,
 - d) duration of the control,
 - e) possible controllers authorised to obtain the data,
 - f) providing information on the rights of the data subjects in connection with the control of the data.
3. Cookies typical of web shops can be classified as so called “cookies used to working process protected with password”, “cookies required to shopping basket” and “security cookies”, which can be used without obtainment of previous consent from the users concerned.
4. Fact of the data control, scope of the controlled data: unique identification number, dates and times
5. Data subjects: all the persons visiting the website.
6. Objective of the data control: Identification of users for keeping a record of the “shopping basket” and tracking the visitors.
7. Duration of the data control, deadline for the data deletion: In the case of session cookies the duration of the data control shall last until the end of browsing the website and in any other case for 1 week.
8. Possible controllers authorized to obtain personal data: By using cookies no control of personal data is performed by the controller.
9. Providing information on the rights of the data subjects in connection with the control of the data: Data subjects may choose to delete cookies in their browser under the setting of the Privacy via the menu item Tools/Settings.
10. Legal grounds for the data control: It is not necessary to obtain consent from the data subject if the cookies are used only for transmission of communication or if it is needed for the service provider to perform the service related to the information society and explicitly requested by the subscriber or user.

Use of Google Adwords Conversion Tracking

1. The controller uses online ad programme called “Google AdWords” and within this the conversion tracking service of Google. The Google conversion tracking is a web analytics service provided by Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; “Google”).
2. When the User accesses any website through a Google ad, then a cookie required to conversion tracking shall be placed on his computer. Validity of such cookies is limited and they do not contain any personal data, consequently, the User cannot be identified by such cookies.
3. While the User is browsing on a website and if the cookie has not expired yet, then both Google and the controller can see that the User has clicked the ad.
4. Each Google AdWords client receives a different cookie, as a result, the cookies cannot be tracked through the websites of the AdWords clients.
5. The information – obtained by means of conversion tracking cookies – shall be used for making conversion statistics for the clients choosing the AdWords conversion tracking. As a result, the clients can receive information about the number of the users clicking their ad and navigated to the website labelled as conversion tracking. On the other hand, they can obtain any information that would enable them to identify any of the users.
6. If you choose not to participate in conversion tracking, you can reject it by blocking the cookies in your browser. Thereafter you will not appear in the conversion tracking statistics.
7. For more information and Google Privacy please visit the website www.google.de/policies/privacy/.

Use of Google Analytics

1. This website uses Google Analytics, which is a web analytics service provided by Google Inc. ("Google"). Google Analytics uses so called "cookies", i.e. text files downloaded to the computer of the user so as to promote analysing the use of the website visited by the User.
2. The information created by the cookies related to website visited by the User is mostly placed and stored on one of the Google servers in the USA. By activating IP anonymisation on the website, the users' IP address is shortened beforehand by Google within member states of the European Union or other contracting states to the Agreement on the European Economic Area.
3. Only in exceptional cases is the full IP address transferred to and shortened by a Google server in the USA. On behalf of the operator of this website, Google will use this information for the purpose of evaluating the users' website use, compiling website activity reports and providing further services relating to website and Internet use to the website operator.
4. The IP address transferred from the users' browser via Google Analytics will not be associated with any other data held by Google. Users can prevent the installation of cookies by selecting the appropriate setting in their browser software; however, the Users should be aware that in this case they might not be able to use all functions of this website to their full extent. Users can also prevent Google from collecting and processing data generated by the cookie about their website use (including their IP address) by downloading and installing a browser plugin accessible via the link <https://tools.google.com/dlpage/gaoptout?hl=hu> .

Newsletter, DM activity

1. Under section 6 of act XLVIII of 2008 on the basic requirements and certain restrictions of commercial advertising activities advertisements may be conveyed to natural persons by way of direct contact through electronic mail or equivalent individual communications only upon the express prior consent of the person to whom the advertisement is addressed.
2. Furthermore, the Client, by taking into consideration the provisions of this Policy, may grant his assent that the Service Provider will control his personal data required to the conveyance of advertisements.
3. The Service Provider shall abstain from sending unsolicited ad offers, and the user shall be entitled to opt out of sending ad offers without limitation and explanation. In such case the Service Provider shall delete the User's personal data – required to sending ad messages – and he shall not send additional ad offers for the User. The User may opt out of the ads by clicking the link provided in the message.
4. Concerning the data control related to newsletters the following terms must be set out in accordance with section 20 (1) of act CXII of 2011 on informational self-determination and freedom of information:
 - a) the fact of the data collection,
 - b) data subjects,
 - c) the objective of the data collection,
 - d) duration of the control,
 - e) possible controllers authorised to obtain the data,
 - f) providing information on the rights of the data subjects in connection with the control of the data.
5. Fact of the data control, scope of the controlled data: name, e-mail address, date and time.
6. Data subjects: all the users subscribing to the newsletter.
7. Objective of the data control: sending electronic mails containing ads for the data subject to provide him with up-to-date information on products, special offers, new functions etc.
8. Duration of the data control, deadline for deletion of the personal data: the data control shall last until the withdrawal of the data subject's consent, i.e. until the opt-out.
9. Possible controllers authorized to obtain personal data: Personal data can be managed by the colleagues of the controller, in compliance with the abovementioned principles.
10. Providing information on the rights of the data subjects in connection with the control of the data: Data subjects may unsubscribe from the newsletter free of charge at any time.

11. Data of the processor (service provider and communication agency) hired during the data control:

Rocket Science Group
675 Ponce De Leon Ave NE #5000,
Atlanta, GA 30308, United States of America

Urban Communications Korlátolt Felelősségű Társaság
Székhely: 2091 Etyek, Mester utca 63.
Adószám: 22641605-2-07
<http://www.urbancomm.hu>

12. Legal grounds for the data control: voluntary consent of the data subject as set out in section 5 (1) of the Information act and section 6 (5) of act XLVIII of 2008 on the basic requirements and certain restrictions of commercial advertising activities:

Advertisers, advertising service providers and publishers of advertising shall keep records on the personal data of persons who provided the statement of consent. The data contained in the aforesaid records relating to the person to whom the advertisement is addressed may be processed only for the purpose defined in the statement of consent, until withdrawn, and may be disclosed to third persons subject to the express prior consent of the person concerned.

Social Networking Websites

1. Concerning the data control of the social networking sites the following terms must be set out in accordance with section 20 (1) of act CXII of 2011 on informational self-determination and freedom of information:
 - a) the fact of the data collection,
 - b) data subjects,
 - c) the objective of the data collection,
 - d) duration of the control,
 - e) possible controllers authorised to obtain the data,
 - f) providing information on the rights of the data subjects in connection with the control of the data.
2. Fact of the data control, scope of the controlled data: name and public profile photo of the user registering on social networking sites such as Facebook/Google+/Twitter/Pinterest/Youtube/Instagram etc.
3. Data subjects: all the users who have registered on social networking sites such as Facebook/Google+/Twitter/Pinterest/Youtube/Instagram etc. and “liked” the site.
4. Objective of the data collection: Sharing, “liking” and popularization of certain content elements, products, special offers of or the website itself.

5. Duration of the data control, deadline for deletion of the controlled data, possible controllers authorized to obtain personal data and providing information on the rights of the data subjects in connection with the control of the data: The data subject can obtain information about the source or control of the data, method and legal grounds of disclosure on the specific social networking site. The data control is carried out on the social networking website, consequently, the duration and method of the data control, or the opportunities to delete or modify personal data shall be regulated by the policy of the specific website.
6. Legal grounds for the data control: voluntary consent of the data subject to the control of his personal data on the social networking sites.

Data Transfer

1. Concerning the data transfer activity of the website the following terms must be set out in accordance with section 20 (1) of act CXII of 2011 on informational self-determination and freedom of information:
 - a) the fact of the data collection,
 - b) data subjects,
 - c) the objective of the data collection,
 - d) duration of the control,
 - e) possible controllers authorised to obtain the data,
 - f) providing information on the rights of the data subjects in connection with the control of the data.
2. Fact of the data control, scope of the controlled data.
 - a) Scope of the transferred data for the delivery: Delivery name, address, telephone number.
 - b) Scope of the transferred data for making the online payment: Invoicing name, address, e-mail address.
3. Data subjects: all the users requesting for home delivery service/online purchase.
4. Objective of the data control: Provision of the home delivery service/online purchase, confirmation of the transactions and fraud-monitoring for protection of the users (controlling of misuses).
5. Duration of the data control, deadline for deletion of personal data: It shall last until the performance of the home delivery/making online payment.
6. Possible controllers authorized to obtain personal data: Personal data may be controlled by the following persons, in compliance with the abovementioned principles:

1138 Budapest, Dunavirág utca 2-6.

ugyfelszolgalat@posta.hu

Telephone: green number 06/80 299 929

In Budapest and surroundings: (06-1) 333-7777

Delivery in the country: (06-1) 333-7777

OTP Bank Zrt.

Registered office: 1051 Budapest, Nádor utca 16.

Tel: 06-1-473-5000

Fax: 06-1-473-5955

<https://www.otpbank.hu/portal/hu/LogiEtikaiNyilatkozat>

7. Providing information on the rights of the data subjects in connection with the control of the data: The data subject may request the controller providing the home delivery service/online payment to delete his personal data the earliest possible.
8. Legal grounds for the data transfer: consent of the User, as set out in section 5 (1) of the Information Act and section 13/A (3) Act CVIII of 2001 on certain issues of electronic commerce services and information society services.

Client Relationships and Other Data Controls

1. Should the data subject have any question or problem arising while using the services of the controller, the data subject may contact the controller by means specified on the website (phone, e-mail, social networking sites etc.).
2. The controller shall delete any e-mail and message received as well as the data provided on Facebook by the enquiring user along with his name and e-mail address or voluntarily provided other personal data not later than within 2 years from the disclosure.
3. We shall inform the data subject about any other case of the data control not specified herein when the personal data are recorded.
4. Upon exceptional official request or in the case of request made by other bodies by statutory authorization the Service Provider shall provide information, disclose personal data or make available documents.
5. In such cases the Service Provider shall disclose as many personal data and to the extent to any requesting body – if it has specified the exact purpose and scope of the data – that is inevitably necessary to the attainment of the objective of the request.

Data Security (Section 7)

1. The controller must plan and execute control operations in a way that these ensure the protection of the privacy of the data subjects.
2. The controller shall ensure data security as well as take technical and organisational measures and develop procedural rules required to enforce the Information Act as well as other data protection and confidentiality rules.
3. Through the institution of the appropriate measures the data must be particularly protected against
 - unauthorised access,
 - modification,
 - transfer,
 - disclosure,
 - deletion or destruction,
 - accidental destruction and damage,
 - disabled access occurring due to changes to the technology applied.
4. In order to protect data sets controlled electronically in various files the controller shall ensure that data stored in files cannot be directly connected and linked to the data subject by ensuring the appropriate technological solutions.
5. In order to prevent any unauthorized access, modification and disclosure of personal data the responsibility of the controller shall cover the following:
 - development and operating of appropriate information and technical environment,
 - controlled selection and supervision of his colleagues participating in the provision of the services,
 - issue of detailed procedures of operating, risk management and services.
6. According to all this above the controller shall ensure that the personal data controlled by him
 - are available for the right holder,
 - authenticity and verification of the personal data are provided,
 - invariance of the personal data can be verified.

7. The IT system of the controller and his web hosting provider shall protect against
 - computer crime,
 - espionage,
 - computer viruses,
 - spam messages,
 - hacking
 - and other attacks.

Rights of Data Subjects

1. The data subject may request the Service Provider to give information on the control of his personal data, correct, delete or block his personal data, with the exception of mandatory data control.
2. Upon request of the data subject the controller is entitled to provide information on the subject's data they control, as well as the data processed by the data processor they contracted, their sources, the objective of the control, its legal grounds and duration, the name and address of the data processor and the activities they undertake in connection with control, in addition to the legal grounds and recipients should the personal data of the data subject not be transferred.
3. The data controller shall keep records to inspect the measures related to data security incidents – by the internal data protection officer, if any – and to inform the data subject, which records shall contain the scope of the personal data and persons affected by the data security incident, the date, conditions, effects and actions taken for prevention of the incident as well as other duties specified in laws prescribing the data control.
4. The controller keeps records of data transferred to verify the legitimacy of the data transfer and informs the data subject which file details the date on which the personal data they controlled was sent, the legal grounds of this action and its recipients, the specific scope of the personal data sent, as well as other data specified in legislation prescribing control.
5. Upon request of the User the Service Provider shall give information on the personal data controlled, on those processed by the data processor they contracted, their sources, the objective of the control, its legal grounds and duration, the name and address of the data processor and the activities they undertake in connection with control, in addition to the legal grounds and recipients should the personal data of the data subject not be transferred. The Service Provider shall give clear information in writing within the shortest possible time following the submission of the request; however, not later than within 25 days. The information shall be provided free of charge.

6. The controller shall correct the personal data if the personal data are not authentic and the controller has access to the authentic personal data.

7. The controller shall block the personal data instead of deletion if the data subject requests him to do so or in the event that the basis of the information available, deletion would presumably violate the rightful interests of the data subject. Personal data blocked through such means may exclusively be controlled while the control objective remains valid which barred the deletion of the personal data.
8. The Service Provider shall delete the personal data if the control thereof is unlawful, it has been requested by the data subject, the personal data are incomplete or incorrect – and this state cannot be remedied according to law, provided that the deletion is not precluded by law, the objective of the control has ceased to exist or the period defined in the relevant legislation for storing the data has expired or if it has been ordered by court or National Authority for Data Protection and Freedom of Information.
9. The controller shall mark the personal data managed by him if the data subject contests the accuracy thereof but the inaccuracy of the personal data cannot be established clearly.
10. The data subject, as well as everyone to whom the data was transferred for control purposes, must be notified of any correction, blocking and deletion. Exemptions apply should this not violate the rightful interest of the data subject in respect of the objective of control.
11. Should the controller fail to fulfil the request of the data subject regarding correction, blocking or deletion, the controller shall provide the reasons and legal grounds for rejecting the request submitted in connection with correction, blocking or deletion within a period of 25 days following the receipt of the request. Should the request for correction, blocking or deletion be rejected, the controller shall notify the data subject of the opportunities available to seek legal redress before the court and on the help available from the Authority.

Legal Redress

1. The data subject is entitled to object to the control of his personal data, if
 - a) the personal data must be controlled or transferred to fulfil the legal obligations of the controller, or validate the rightful interests of the controller, data recipient or third party except in the case of mandatory data control;
 - b) the personal data are used or transferred directly for business benefits, public opinion surveys or scientific research purposes, or
 - c) in other cases defined in relevant legislation.
1. The Service Provider shall assess the objection lodged within the shortest possible time limit following the submission of the request; however, he shall assess the document within a maximum period of 15 days and make a decision on the grounds of the objection and notify the applicant of the decision in writing. Should the

controller find the objection lodged by the data subject well-grounded, the controller shall suspend the control process – including data entry and data transfer – block the data and notify everyone to whom the personal data constituting the object of objection have been transferred, as well as measures taken on the grounds of this, which individuals are obliged to take measures to enforce the right to object.

2. If the data subject disagrees with the decision made by the controller, the data subject may initiate legal proceedings against the decision within 30 days of the notification. The court shall take immediate action in such cases.
3. The data subject is entitled to lodge a complaint against possible infringement by the controller to the National Authority for Data Protection and Freedom of Information:

National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság)
 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
 Mailing address: 1530 Budapest, Postafiók: 5.
 Telephone: +36 -1-391-1400
 Fax: +36-1-391-1410
 E-mail: ugyfelszolgalat@naih.hu

Judicial enforcement

1. The controller shall prove that the personal data have been controlled in compliance with the relevant legislation. The obligation to prove the legality of the data transfer shall be borne by the data recipient.
2. Judgement of the case shall fall within the scope of the jurisdiction of the County Court. The legal procedure may be initiated at the county court competent in the place of residence of the data subject, according to his choice of court.
3. Persons normally not having the capacity to be a party to legal proceedings may also be parties to the litigation. The Authority is entitled to intervene in the proceeding in favour of the data subject.
4. If the court sustains the objection, the controller shall be obliged to provide information, correct, block and delete the data, invalidate the decision made with the help of automated data processing, to take into consideration the data subject's right to object and disclose the data requested by the data recipient.
5. In case the data recipient's motion is rejected by the court, the controller shall delete the personal data of the data subject within 3 days following the notification of the judgement. The controller shall also delete the personal data if the data recipient fails to go to court within the specified time limit.
6. The court may order the disclosure of its judgement – by disclosing the controller's ID data – if this is required in the interest of data protection and the rights of a higher number of data subjects to be protected.

Indemnification and Compensation for Injury to Feelings

1. If the controller violates the personal rights of the data subject by unlawful control of his personal data or by violating the requirements of data security, the data subject may require compensation for injury of feelings from the controller.
2. The controller shall be liable for damages caused by the data processor against the data subject, and the data controller shall also pay compensation for injury of feelings due to the data subject in the case of violation of personal rights caused by the data processor. The data controller shall be exempted from the liability and obligation to pay compensation for injury of feelings if he can prove that the damages were caused by circumstances beyond the immediate control.
3. No damage shall be compensated for and no compensation for injury of feelings shall be paid if the damage or infringement caused by violating the personal rights has arisen from the deliberate act or gross negligence of the data subject incurring the damage.

Closing remarks

We have prepared this Privacy Policy by taking into consideration the following laws:

- Act CXII of 2011 on informational self-determination and freedom of information (hereinafter: Information Act)
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services (particularly Section 13/A)
- Act XLVII of 2008 on the prohibition of unfair commercial practices against consumers;
- Act XLVIII of 2008 on the basic requirements and certain restrictions of commercial advertising activities (in particular, Section 6)
- Act XC of 2005 on the freedom of electronic information
- Act C of 2003 on electronic communications (specifically Section 155)
- Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online
- Recommendation of the National Data Protection and Freedom of Information Authority on the requirements to be taken into consideration when preparing data processing information documents