

Webshop.bock.hu

Privacy Statement

In Short

We collect and manage personal data only in accordance with the law.

We send DM letters only under specific consent. We may send system messages also in lack of such consent.

We store the data in the safest possible way.

We disclose personal data to third parties only upon express consent.

We shall provide information to the data subjects about the data stored concerning them, and they may also request the erasure of their data at any time by contacting us.

Introduction

The company **Bock Panzió Kft.** (registered office: H-7773 Villány, Batthyány u. 15, tax number: 13855264-2-02) (hereinafter referred to as: 'Service Provider' or 'data controller') undertakes to be bound by the provisions of the following statement.

Section 20 (1) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information provides that prior to data management being initiated, the data subject (in this case the user of the webshop, hereinafter: 'user') shall be informed whether their **consent is required** or management is mandatory.

Before the commencement of data management, the data subject shall be clearly and elaborately informed of all aspects concerning the management of their personal data, such as the **purpose** for which their data is required and the **legal basis**, the **person entitled to control the data and to carry out the processing**, and the **duration** of the proposed data management.

Pursuant to Section 6 (1) of the Info Act, the data subject shall also be informed that personal data may be managed also if obtaining the data subject's consent is impossible or it would give rise to disproportionate costs, and the management of personal data is necessary

- for compliance with a legal obligation pertaining to the data controller, or
- for the purposes of the legitimate interests pursued by the data controller or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data.

Information shall also be provided on the data subject's rights and remedies relating to data management.

If the provision of personal information to the data subject is impossible or would involve disproportionate costs (such in this case in a webshop), the obligation of information may be satisfied by the public disclosure of the following:

- a) an indication of the fact that data is being collected,
- b) the scope of data subjects,
- c) the purpose of data collection,
- d) the duration of data management,
- e) the potential data controllers with right of access,
- f) presentation of the rights of data subjects and remedies available relating to data management; and
- g) where the management of data has to be registered, the number assigned in the data protection register.

This Privacy Statement regulates the data management operations carried out in connection with the <https://webshop.bock.hu> website, and is based on the above requirement relating to content. The Statement is available at <https://webshop.bock.hu/adatvedelem>

Any amendments to the Statement shall take effect upon being published on the above website.

Definitions *(Section 3)*

1. *'data subject'/'User'* means any specific natural person identified or – directly or indirectly – identifiable by reference to personal data;
2. *'personal data'* means data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to their physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject;
3. *'data controller'* means a natural or legal person, or organisation without legal personality which alone or jointly with others determines the purposes and means of the management of data; makes and executes decisions concerning data management (including the means used) or has it executed by a data processor;
4. *'data management'* means any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, erasing and destructing the data, as well as preventing their further use, 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'* means performing technical tasks in connection with data management operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data;
6. *'data processor'* means any natural or legal person or organisation without legal personality processing the data on the grounds of a contract concluded with the data controller, including contracts concluded pursuant to legislative provisions;
7. *'data incident'* means the unlawful management or processing of the personal data, thus in particular unauthorized access, alteration, transfer, disclosure to the public, erasure or destruction, accidental destruction and compromise.

Management of Data in Connection with the Operation of the Webshop

1. Pursuant to Section 20 (1) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information, the following shall be specified in the scope of data management relating to the operation of the webshop:

- a) an indication of the fact that data is being collected;
- b) the scope of data subjects,
- c) the purpose of data collection,
- d) the duration of data management,
- e) the potential data controllers with right of access,
- f) presentation of the rights of data subjects available relating to data management.

2. The fact of data collection, the scope of the data managed, and the purpose of data management:

| Personal data | Purpose of data management |
|---|--|
| Password | Secure login to the user account. |
| Surname and first name | Necessary for communication, purchase and the issue of proper invoices. |
| Email address | Communication |
| Telephone number | Communication, effective consultation in the issues concerning invoicing and delivery. |
| Invoicing name and address | Issue of proper invoices, conclusion of the contract, determination and amendment of the content thereof, monitoring performance of the contract, invoicing the relevant fees, enforcement of the relevant claims. |
| Delivery name and address | Home delivery. |
| Date and time of purchase/registration | Performance of technical operations. |
| IP address used for purchase/registration | Performance of technical operations. |

Neither the username nor the email address shall necessarily contain personal data.

3. The scope of data subjects: All data subjects who have registered/purchased a product in the webshop.
4. Duration of data management, deadline for erasure of the data: Immediately upon the deletion of registration. Except for accounting documents, as these data shall be kept on file for 8 years pursuant to Section 169 (2) of Act C of 2000 on Accounting.

The accounting documents underlying the accounting records directly or indirectly (including ledger accounts, analytical records and registers) shall be retained for minimum eight years, shall be legible and retrievable by means of the code of reference indicated in the accounting records.

5. Potential data controllers with right of access: The personal data may be managed by the data controller's sales and marketing personnel, by honouring the above principles.
6. Presentation of the rights of data subjects available relating to data management: The following data can be modified on the websites: password, surname and first name, email address, telephone number, delivery address, delivery name, invoicing address, invoicing name. The data subject can initiate the erasure or alteration of their personal data the following way:
 - by post at the address of H-7773 Villány, Batthyány u. 15,
 - by email at the webshop@bock.hu email address,
 - by telephone at the +36 72 492 919 or +36 30 9975 600 telephone number.
7. The data of data processors used in the course of data management:

Web design (image and graphic design)

2Pixels Studio

Mobile: +36 70 3691 391

Email: info@2pixels.hu

Web: 2pixels.hu

Web development (programming and technical operation)

Bábelhal Webstudio

Mobile: +36 20 3888 458

Email: info@babelhal.hu

Web: babelhal.hu

Web hosting

Bábelhal Webstudio Kft.

H-8360 Keszthely, Honvéd utca 17/2

Telephone: +36 83 777 603

Email: info@babelhal.hu

8. The legal basis for data management is: the User's consent, Section 5 (1) of the Info Act, and Section 13/A (3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce Activities and Information Society Services (hereinafter: Electronic Commerce Act):

In order to render the service, the service provider may manage those personal data that are technically indispensable for the provision of the service. In circumstances where other conditions are identical, the service provider shall select and operate the tools used for rendering the information society services in such a way as to ensure that personal data are not managed unless if it is indispensable for the provision of the service and the fulfilment of the purposes specified in this act, and even in such cases, only to the extent and for the duration as necessary.

Management of Cookies

1. Pursuant to Section 20 (1) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information, the following shall be specified in the scope of the management of data relating to the cookies used in the webshop:
 - a) an indication of the fact that data is being collected,
 - b) the scope of data subjects,
 - c) the purpose of data collection,
 - d) the duration of data management,
 - e) the potential data controllers with right of access,
 - f) presentation of the rights of data subjects available relating to data management.
2. Webshops typically use cookies such as the so-called 'password-protected session cookies', 'shopping cart cookies' and 'security cookies' the use of which does not require previous consent from the data subjects.
3. The fact of data management, scope of the data managed: Unique identifier, dates, times
4. The scope of data subjects: All data subjects visiting the website.
5. Purpose of data management: Identification of users, registration of the 'shopping cart' and monitoring of visitors.
6. Duration of data management, deadline for erasure of the data: In case of session cookies, data are managed until the end of the user's visit on the website, while in other cases for no more than two years.
7. Potential data controllers with right of access: The use of cookies does not involve the management of personal data by the data controller.
8. Presentation of the rights of data subjects available relating to data management: Data subjects can delete cookies in the Tools/Settings menu of their browser, generally among the settings of the Privacy menu.
9. Legal basis for data management: The data subject's consent is not required if the exclusive purpose of using cookies is to communicate through the electronic communications network, or its use is indispensable for the service provider to render an information society service expressly requested by the subscriber or the user.

Use of Google Adwords Conversion Tracking

1. The data controller uses the 'Google AdWords' online advertising program, including Google's conversion tracking service. Google conversion tracking is an analysis service offered by Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; 'Google').
2. If a User visits a website through a Google-ad, a conversion tracking cookie is deposited on his or her computer. These cookies have limited validity and they do not contain any personal data, and therefore cannot be used for the User's identification.
3. If the User visits certain pages on the website and the cookie has not yet expired, both Google and the data controller can detect that the User has clicked on the advertisement.
4. Each Google AdWords customer receives a different cookie, and so the cookies cannot be traced back via the websites of AdWords customers.
5. The information obtained using the conversion cookie is used to generate conversion statistics for AdWords customers. This way customers are given a number of users who have clicked on their advertisement and proceeded to a page tagged with a conversion tracking tag. However, they will not receive any information that can be used to personally identify users.
6. If you want to opt out of conversion tracking, you can reject it by disabling the installation of cookies in your browser. After that, you will not be included in conversion tracking statistics.
7. More information and Google's Privacy Policy is available at: www.google.de/policies/privacy/

Use of Google Analytics

1. This website uses Google Analytics, a web analytics service offered by Google, Inc. ('Google'). Google Analytics uses 'cookies' that are text files placed on the User's computer and which help analyse how Users use the site.
2. The information generated by the cookie about the User's use of the website is generally transmitted to and stored by Google on servers in the USA. If, however, IP anonymisation is activated on the website, Google will beforehand shorten the User's IP address within Member States of the European Union or in other states that are party to the Agreement on the European Economic Area.
3. Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and shortened there. Google will use this information on behalf of the operator of this website to evaluate the User's use of the website, to compile reports on the website activities and to provide further services associated with the use of the website and the Internet for the website operator.
4. The IP address that the User's browser transmits as part of Google Analytics will not be associated with any other data held by Google. The User can prevent the storage of cookies by selecting the corresponding setting in his or her browser, but please note that in such a case the User may not be able to use all the functions on this website. The User can also prevent Google's collection and use of data generated by the cookie and related to the User's use of the website (including the User's IP address) as well as the processing of this data by downloading and installing the browser plugin available at <https://tools.google.com/dlpage/gaoptout?hl=hu>

Newsletter, DM activity

1. Pursuant to Section 6 of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, the User may grant their prior and express consent to the Service Provider sending them promotional offers or other messages to their contact information provided during registration.
2. Bearing in mind the provisions of this Statement, the Customer may also consent to the Service Provider managing their data necessary for sending the promotional offers.
3. The Service Provider will not send unsolicited promotional messages, and the User may unsubscribe from the notifications without restriction, free of charge and without having to give the reasons. In such a case the Service Provider will erase all of the User's personal data – that are necessary for the sending of promotional messages – from its records, and will not send further promotional messages to the User. The User can unsubscribe from advertisements by clicking on the link in the message.
4. Pursuant to Section 20 (1) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information, the following shall be specified in the scope of the data managed in relation to newsletters:
 - a) an indication of the fact that data is being collected,
 - b) the scope of data subjects,
 - c) the purpose of data collection,
 - d) the duration of data management,
 - e) the potential data controllers with right of access,
 - f) presentation of the rights of data subjects available relating to data management.
5. The fact of data management, scope of the data managed: name, email address, date, time.
6. The scope of data subjects: All data subjects who have subscribed to newsletter.

7. Purpose of data management: to send electronic messages containing advertisements to the data subject, and to provide information about current news, products, promotions, new functions etc.
8. Duration of data management, deadline for erasure of the data: until cancellation of the consent i.e. until the cancellation of subscription.
9. Potential data controllers with right of access: The personal data may be managed by the data controller's personnel, by honouring the above principles.
10. Registration number of the data management: NAIH-116184/2017.
11. Presentation of the rights of data subjects available relating to data management: The data subject may unsubscribe from the newsletter at any time, free of charge.
12. The data processor used in the course of data management:

MailChimp
The Rocket Science Group, LLC
675 Ponce de Leon Ave NE
Suite 5000
Atlanta, GA 30308 USA

13. The legal basis for data management is: the data subject's voluntary consent, Section 5 (1) of the Info 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 maintain records on the personal data of persons who provided the statement of consent to the extent specified in the statement. 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 affected.

Social Media Sites

1. Pursuant to Section 20 (1) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information, the following shall be specified in the scope of the data managed by social media sites:
 - a) an indication of the fact that data is being collected,
 - b) the scope of data subjects,
 - c) the purpose of data collection,
 - d) the duration of data management,
 - e) the potential data controllers with right of access,

- f) presentation of the rights of data subjects available relating to data management.
2. The fact of data collection, the scope of the data managed: The user's name as registered on Facebook/Google+/Twitter/Pinterest/Youtube/Instagram or other social media sites, and the user's public profile picture.
 3. The scope of data subjects: All data subjects who have signed up for Facebook/Google+/Twitter/Pinterest/Youtube/Instagram or other social media sites and have 'liked' the website.
 4. The purpose of data collection: To share certain content elements of the website, or the products and promotions on the website or the website itself on these social media sites, and to promote the same, so that users 'like' them.
 5. Duration of data management, deadline for erasure of the data, the potential data controllers with right of access, and presentation of the rights of data subjects available relating to data management: The data subject can obtain information regarding the source and management of the data, as well as the manner of and legal basis for data transfer on the social media site in question. Data management is performed on the social media sites, and so the duration and method of data management, as well as the possibilities of erasure and alteration of the data are governed by the policies of the given social media site.
 6. Legal basis for data management: the data subject's voluntary consent to the management of their data on the social media sites.

Data Transfer

1. Pursuant to Section 20 (1) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information, the following shall be specified in the scope of the data transfer activities of the webshop:
 - a) an indication of the fact that data is being collected,
 - b) the scope of data subjects,
 - c) the purpose of data collection,
 - d) the duration of data management,
 - e) the potential data controllers with right of access,
 - f) presentation of the rights of data subjects available relating to data management.
2. The fact of data management, scope of the data managed:
 - a) The scope of data transferred in order to perform delivery: Delivery name, delivery address, telephone number.

- b) The scope of data transferred in order to administer online payment:
Invoicing name, invoicing address, email address.
3. The scope of data subjects: All data subjects requesting home delivery/online purchase.
 4. Purpose of data management: Home delivery of the ordered product/the administration of online purchase, fraud-monitoring to confirm transactions and protect users.
 5. Duration of data management, deadline for erasure of the data: Until the completion of home delivery/online purchase.
 6. Potential data controllers with right of access: The following entities may manage the personal data, by honouring the above principles:

MPL Magyar Posta Logisztika Kft.

H-1138 Budapest, Dunavirág utca 2-6

ugyfelszolgalat@posta.hu

Telephone: (+36-1) 333-7777

GTC: <https://www.posta.hu/ugyfelszolgalat/aszf>

Privacy Statement: https://www.posta.hu/adatkezelesi_tajekoztato

TNT Express Hungary Kft.

registered office: H-1094 Budapest, Ecséri út 14-16

Telephone: +36 40 31 3131

email: HU.TNTEXPRESS@TNT.COM

Privacy Statement:

http://www.tnt.com/express/hu_hu/site/privacy_statement.html

Cib Bank Zrt.

Address: 1027 BUDAPEST, MEDVE U. 4-14

Mailing address: H-1537 Budapest, PO Box (Pf.) 394

Telephone number: (+36-1) 423-1000

Email cím: cib@cib.hu

Web: www.cib.hu

Privacy Statement: http://www.cib.hu/jogi_nyilatkozat/index

PayPal

Parent company: eBay Incorporated

Registered office: San Jose, California, USA

Contact: <https://www.paypal.com/hu>

Privacy Statement: [https://www.paypal.com/hu/cgi-bin/helpscr?](https://www.paypal.com/hu/cgi-bin/helpscr?cmd=p/gen/ua/policy_privacy-outside)

[cmd=p/gen/ua/policy_privacy-outside](https://www.paypal.com/hu/cgi-bin/helpscr?cmd=p/gen/ua/policy_privacy-outside)

7. Presentation of the rights of data subjects available relating to data management: The data subject may request the data controller performing the home delivery/online purchase service to erase their data as soon as possible.
8. The legal basis for data transfer is: the User's consent, Section 5 (1) of the Info Act, and Section 13/A (3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce Activities and Information Society Services.

Customer Relations and Other Data Management

1. If the data subject has any questions or problems during their use of the data controller's services, they can contact the data controller at its contact information (phone, email, social media sites etc.) specified on the website.
2. The emails and messages received, the data provided by telephone or via Facebook etc., including the name, email address and any other voluntarily provided personal data of the data subject will be erased by the data controller within a maximum of 2 years from the date of provision.
3. Regarding any type of data management not listed herein, we will provide information at the time of recording the data in question.
4. In exceptional cases at the authorities' request, or at the request of other bodies authorised by law, the Service Provider may be obliged to provide information, disclose and transfer data, or supply documents.
5. In such cases, provided that the requesting entity has specified the exact purpose of use and the scope of the data, the Service Provider will only disclose those personal data to the requesting entity and only to such extent that is indispensable for the implementation of the purpose of the request.

Data Security (Section 7)

1. The data controller shall design and implement data management operations in such a manner so as to ensure protection of the data subjects' privacy.
2. The data controller shall provide for the security of the data (SSL encryption, antivirus protection), take the technical and organisational measures and have procedures in place that are necessary for the enforcement of the Info Act and other rules concerning the protection of data and secrets.

3. The data controller is using appropriate measures to protect the data in particular against
 - unauthorised access,
 - alteration,
 - transfer,
 - disclosure to the public,
 - erasure or destruction,
 - accidental destruction and damage,
 - and to ensure that data cannot be rendered inaccessible due to any changes in the technology applied.
4. The data controller has suitable technical solutions in place to prevent the interconnection of data stored in the filing systems and the identification of the data subjects.
5. In order to prevent unauthorised access to the personal data, as well as the alteration, unauthorised disclosure or use of the data, the data controller shall ensure to:
 - design and operate a proper IT and technical environment,
 - controllably recruit and supervise its employees participating in the rendering of the services,
 - issue detailed policies on operation, risk management and service provision.
6. According to the above, regarding the data managed by it, the service provider shall ensure that
 - the data are available to the entities authorised to access the same,
 - they are authentic and authenticated,
 - it can be certified that the data have not been altered.
7. The IT system used by the data controller and its hosting provider shall provide protection against (including but not limited to) the following:
 - computer fraud,
 - spying,
 - computer viruses,
 - spams,
 - hacks,
 - and other attacks.

The Rights of Data Subjects

1. The data subject may request the Service Provider to provide information on their personal data being processed, may request the rectification of their personal data, and may request the erasure or blocking of their personal data, save where data management is rendered mandatory.
2. Upon the data subject's request the data controller shall provide information concerning the data managed by the controller regarding the data subject, including those processed by a data processor on its behalf, the sources from where they were obtained, the purpose, grounds and duration of management, the name and address of the data processor and its activities relating to data management, the circumstances and effects of any data incident, along with the measures taken for elimination, and – if the personal data of the data subject is transferred to others – the relating legal basis and the recipient.
3. Data controllers – by means of an internal data protection officer should they have appointed one and with a view to control measures relating to data incidents and to inform data subjects – shall keep records containing the personal data affected, the personal scope affected by the data incident, the time, circumstances and effects of the data incident and measures taken to eliminate the same, as well as other information determined by law.
4. With a view to verifying legitimacy of data transfer and for the information of the data subject, the data controller shall maintain a transmission log, showing the date and time of transmission, the legal basis of transmission and the recipient, description of the personal data transmitted, and other information prescribed by the relevant legislation on data management.
5. Upon the data subject's request the data controller shall provide information of the data managed by the data controller, the sources from where they were obtained, the purpose, grounds and duration of management, the name and address of the data processor and its activities relating to data management, and – if the personal data of the data subject is transferred to others – the relating legal basis and the recipient. The Service Provider must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing, within not more than twenty-five days. The information shall be provided free of charge.
6. Where a personal data is deemed inaccurate, and the correct personal data is at the data controller's disposal, the data controller shall rectify the personal data in question.
7. The Service Provider will block the personal data instead of erasure if so requested by the User, or if there are reasonable grounds to believe that erasure could affect the legitimate interests of the User. The personal data blocked may be managed only for so long as the data management purpose preventing the erasure exists.
8. The Service Provider shall erase the personal data if they are managed unlawfully, the User so requests, the managed data are incomplete or inaccurate – and this cannot be lawfully remedied, provided that erasure is not disallowed by a statutory

provision of an act –, the purpose of data management no longer exists or the legal time limit for storage has expired, or if so ordered by court or by the Hungarian National Authority for Data Protection and Freedom of Information.

9. If the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained beyond doubt, the data controller shall mark that personal data for the purpose of referencing.
10. When a data is rectified, blocked, marked or erased, the data subject and all recipients to whom it was transmitted for management shall be notified. Notification is not required if it does not violate the rightful interest of the data subject in light of the purpose of management.
11. If the data controller refuses to comply with the data subject's request for rectification, blocking or erasure, the factual or legal reasons on which the decision for refusing the request for rectification, blocking or erasure is based shall be communicated in writing within twenty-five days of receipt of the request. Where rectification, blocking or erasure is refused, the data controller shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority.

Remedy

1. The User may object to the management of his or her personal data
 - a) if the management or transfer of the personal data is necessary exclusively for the performance of the Service Provider's legal obligation or for enforcing the legitimate interests of the Service Provider, the data recipient or a third party, except if the management of the data is ordered by law;
 - b) if the personal data are used or transferred for the purposes of direct marketing, opinion polling or scientific research;
 - c) in other cases provided for by law.
2. In the event of objection, the Service Provider shall investigate the cause of objection within the shortest possible time inside a fifteen-day time period, adopt a decision as to whether it is well-founded and shall notify the data subject in writing of its decision. If, according to the findings of the Service Provider, the data subject's objection is justified, the Service Provider shall terminate all data management operations (including data collection and transfer), block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.
3. If the User disagrees with the decision taken by the Service Provider, the User shall have the right to turn to court within thirty days of the date of delivery of the decision. The court shall hear such cases in priority proceedings.

4. Complaints may be filed against the data controller's violation of law, if any, with the Hungarian National Authority for Data Protection and Freedom of Information:

Hungarian National Authority for Data Protection and Freedom of Information
1125 Budapest, Szilágyi Erzsébet fasor 22/C
Mailing address: H-1530 Budapest, PO Box (Pf.) 5
Telephone: +36 -1-391-1400
Fax: +36-1-391-1410
Email: ugyfelszolgalat@naih.hu

Judicial Remedy

1. The burden of proof to show compliance with the law lies with the data controller. The burden of proof concerning the lawfulness of transfer of data lies with the data recipient.
2. The action shall be heard by the competent tribunal. If so requested by the data subject, the action may be brought before the tribunal in whose jurisdiction the data subject's home address or temporary residence is located.
3. Any person otherwise lacking legal capacity to be a party to legal proceedings may also be a party in such actions. The Authority may intervene in the action in the data subject's interest.
4. When the court's decision is in favour of the plaintiff, the court shall order the controller to provide the information, to rectify, block or erase the data in question, to annul the decision adopted by means of automated data-processing systems, to respect the data subject's objection, or to disclose the data requested by the data recipient.
5. If the court rejects the petition filed by the data recipient, the controller shall be required to erase the data subject's personal data within three days of delivery of the court ruling. The data controller shall erase the data even if the data recipient does not file for court action within the specified time limit.
6. The court may order publication of its decision, indicating the identification data of the data controller as well, where this is deemed necessary for reasons of data protection or in connection with the rights of large numbers of protected data subjects.

Compensation and Restitution

1. If the data controller, by unlawful management of the data subject's data or by breaching data security rules, violates the personal rights of the data subject, the latter may demand restitution from the data controller.
2. The data controller shall be liable for the damage caused by the data processor and it will be liable to pay restitution for personal rights violations as well. The controller shall be released from liability for damages and from paying restitution if it demonstrates that the damage or the violation of personal rights were brought about by unavoidable reasons beyond its data management activity.
3. No compensation shall be paid and no restitution shall be demanded where the damage or the violation of rights was caused by intentional or serious negligent conduct on the part of the aggrieved party or the data subject.

Closing Remarks

When preparing the information we took into account the provisions of the following laws:

- Act CXII of 2011 – on Informational Self-Determination and Freedom of Information (hereinafter: Info Act)
- Act CVIII of 2001 – on Certain Issues of Electronic Commerce Activities and Information Society Services (Section 13/A in particular)
- Act XLVII on 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 (Section 6 in particular)
- Act XC of 2005 on the Freedom of Information by Electronic Means
- Act C of 2003 on Electronic Communications (Section 155 in particular)
- Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising
- Recommendation by the Hungarian National Authority for Data Protection and Freedom of Information on the Date Protection Requirements of Prior Information