PRIVACY NOTICE
FOR GUESTS AND USERS OF THE WEBSITE
CONCERNING THE PROCESSING OF THEIR PERSONAL DATA

Controller: **Inter-Deversor Kft., as the operator of Inter Hotel*****
Company registration number: 09-09-034946
VAT number: 32228456-2-09
Registered seat: 4032 Debrecen, Gyimes utca 4.
Website: www.interhotel.hu
Email: inter.deversor@gmail.com

1. General Information

Aim of this Privacy Notice:

The primary aim of this notice is to provide information on the Controller's data protection and data processing principles and rules regulating the processing of the personal data of natural persons contacting the Controller.

When drafting the provisions of this privacy notice, the Controller especially took into account the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter: GDPR), Act CXII of 2011 on informational self-determination and freedom of information (hereinafter: Privacy Act) and other relevant legal regulations.

2. TERMS RELATED TO DATA PROCESSING

The definitions used in the processing of personal data are specified by the GDPR. For transparency and clarity, the Controller stipulates the most important terms in this section by using the definitions of the GDPR.

1. **"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, an identification 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;
2. "**Special Personal Data**" are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data,

biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. As a rule, the processing of such data is prohibited.

3. "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
4. "**Restriction of Processing**" means the marking of stored personal data with the aim of limiting their processing in the future;
5. "**Controller**" means the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
6. "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
7. "**Recipient**" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
8. "**Third Party**" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
9. "**Consent of the Data Subject**" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
10. "**Enterprise**" means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
11. "**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;
12. "**Supervisory Authority**" means an independent public authority which is established by a Member State pursuant to Article 51.

3. THE PRINCIPLES OF PROCESSING

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
- Personal data may only be processed for specified and legitimate purposes, for exercising rights and performing obligations.
- Processing shall comply with the purpose in all stages, the recording and processing of data shall be fair and lawful. Only those personal data may be processed which are inevitable for fulfilling the purpose of processing and are suitable for achieving such purpose.
- Personal data may only be processed to the extent and for the period necessary for achieving the purpose.
- Processing by the Controller is accurate and up to date. The Controller shall take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- The Controller shall keep personal data 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, taking into account the storage obligations specified by the legal regulations.
- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- The Controller shall be responsible for, and be able to demonstrate compliance with the aforesaid principles.

4. PURPOSE, LEGAL BASIS, DURATION AND MEANS OF PROCESSING

4.1. Contacting and booking by email and online contact or booking form

Purpose of processing: based on the Data Subject's query, contacting and communicating with the Data Subject, and in case of request for quotation, sending the accurate, customized quotation. The Controller uses the data provided by the Data Subject for a limited purpose, only for contacting the Data Subject. Unless there is a binding legal regulation governing this, personal data may only be provided to third parties with the Data Subject's prior express consent.

Legal basis of processing: pursuant to Article (6) (1) a) of the GDPR, the freely given consent of the Data Subject
Data processing is performed on the basis of the freely given, informed consent of the Data Subject, which is given by the Data Subject by sending the query and the data contained in it to the Controller for the purpose of answering the query and arranging the related requests (e.g. providing information, sending the accurate quotation).

The Data Subject gives his/her consent by providing the concerned data freely, and in case of a form, by ticking the relevant checkbox.

Processed personal data:

- name (first name and family name)
- email address
- phone number
- address
- arrival and departure data
- number of persons (adults and/or children).

The Controller does not check the received personal data. The person providing such data shall be exclusively responsible for the truthfulness of the data.

Duration and means of processing

Data processing is performed electronically.

Within the framework of contacting and communication, the provided personal data are processed:

- until the Data Subject withdraws the consent,
- or for one year from the date of providing the data at the latest, electronically.

In relation to booking, for eight years following the payment of the advance deposit (irrespectively of the date of a potential cancellation) pursuant to Section 169 (2) of the Accounting Act.

4.2 Contacting via Facebook

Purpose of processing: for offering an option for online contacting, for publishing posts, for advertising the enterprise and reaching the potential clients, the Controller operates a Facebook page (https://www.facebook.com/profile.php?id=100092882911043)

When commenting the posts of the enterprise, the Controller learns the first and family names and the comments of the commenters, which are accessed on the basis of consent.

Messages may also be sent on the Facebook page. During messaging, the Controller learns the first and family names of the senders, which are accessed on the basis of the sender's consent. In case of contacting in the form of Facebook messages, the Controller informs the data subject in writing that bookings may only be made by email, on the website or personally.

Furthermore, the Controller informs the Data Subject in writing about this privacy notice and draws the attention of the sender to the fact that his/her personal data may only be processed if the sender confirms in writing that he/she has learned and accepted the contents of this notice.

Legal basis of processing: pursuant to Article (6) (1) a) of the GDPR, the freely given consent of the Data Subject

The Controller does not process the personal data disclosed by the visitors of its Facebook page.

Processing is performed on the social media website, and therefore, the duration, means of processing, as well as the possibilities of erasing and modifying data are governed by the regulations of the given social media site.

The privacy notice of Facebook and Instagram (as Meta products) is available at the following link: https://www.facebook.com/privacy/explanation.

A direct link leads to this notice in the impressum menu of Facebook (Insights data/Privacy/Terms).

Processed personal data:

- registered name of the user on Facebook social media site
- and the public profile photo of the user

The Controller does not check the received personal data. The person providing such data shall be exclusively responsible for the truthfulness of the data.

Duration and means of processing

Within the framework of contacting and communication, the processing of the provided personal data is performed electronically until the data subject withdraws his/her consent, and if no client relationship is established between the Controller and the Data Subject, the Controller deletes all data related to contacting without delay on the basis of the erasure options provided by Facebook.

4.3. Personal booking

Purpose of processing: the Data Subject may also book accommodation at the Hotel reception. The Controller uses the data provided by the Data Subject for a limited purpose, only for contacting the Data Subject. Unless there is a binding legal regulation governing this, personal data may only be provided to third parties with the Data Subject's prior express consent.

Legal basis of processing: pursuant to Article (6) (1) a) of the GDPR, the freely given consent of the Data Subject

Data processing is performed on the basis of the freely given, informed consent of the Data Subject, which is given by the Data Subject by contacting and providing his/her data to the Controller.

The Controller informs the Data Subject on the availability this notice.

Processed personal data:

- name (first name and family name)
- email address
- phone number
- address
- arrival and departure data
- number of persons (adults and/or children).

The Controller does not check the received personal data. The person providing such data shall be exclusively responsible for the truthfulness of the data.

Duration and means of processing

Data processing is performed electronically.

Within the framework of contacting and communication, the provided personal data are processed:

- until the Data Subject withdraws the consent,
- or for one year from the date of providing the data at the latest, electronically.

In relation to booking, for eight years following the payment of the advance deposit (irrespectively of the date of a potential cancellation) pursuant to Section 169 (2) of the Accounting Act.

4.4. Booking via booking.com portal

Purpose of processing: registration of bookings made via the booking portal, and following booking, providing the account number for collecting the advance deposit.

Legal basis of processing: pursuant to Article (6) (1) a) of the GDPR, the freely given consent of the Data Subject

Processed personal data:

Data Subjects: all natural persons booking accommodation via the website or any of the accommodation portals.

Processed personal data:

- name (first name and family name)
- email address
- phone number
- address
- arrival and departure data
- number of persons (adults and/or children)
- bank/credit card data.

Duration and means of processing:

Data processing is performed electronically.
In relation to booking, for eight years following the payment of the advance deposit (irrespectively of the date of a potential cancellation) pursuant to Section 169 (2) of the Accounting Act.

The Controller draws the attention of the Data Subjects to the fact that *booking.com* portal *(on which bookings can be made for the accommodation operated by the Controller via its own website)* **is a separate controller, independent from the Controller. Accordingly, we hereby request you to obtain information on the data processing principles and regulations of the booking portal on its website mentioned below.**

booking.com:
https://www.booking.com/content/privacy.hu.html?aid=397634;label=gog235jc-index-hu-XX-XX-unspec-hu-com-L%3Ahu-V%3A0ahUKEwj5ja6PkcfbAhWCxaYKHUYoD0IQFggwMAA-O%3Aabn-B%3AinternetSexplorer-N%3AXX-S%3Abo-U%3Ac-H%3As;sid=a46fbeb0970b7e81cebecc925923e394

5. CHECK-IN

Purpose of processing: identification and compliance with legal obligations.

When arriving, the Data Subject fills in an online check-in form before getting the room (https://interhotel.hu/self-check-in/). The Controller processes the received data for performing its obligations set out in the relevant legal regulations, for certifying performance and for identifying the Guest.

The National Tourism Data Supply Centre (NTDSC) is a digital data supply system operated by the Hungarian Tourism Agency (HTA) allowing real-time monitoring of the traffic and statistics data of all accommodation establishments in Hungary.
All accommodation providers can fulfil their data registration obligations required for checking in the guests digitally, by using the accommodation management software. The NTDSC receives data from the accommodation providers in the form of direct data

connection, and then stores and processes such data, prepares aggregated and structured reports, analyses, and provides these to the data suppliers of the sector and to the authorities specified by law.

Legal basis of processing: Article 6 (1) c) of the GDPR, and Section 9/H of Act CLVI of 2016 on state functions pertaining to the development of tourism regions

Processed personal data:

The following data of the person using the services of the accommodation provider:

- first name and family name,
- place and date of birth
- mother's maiden name and family name,
- residential address
- data of the documents suitable for identification and of travel documents, in case of citizens of third countries, the number of visa or residence permit, place and date of entry,
- address of the accommodation provider, the start and expected end dates of using the accommodation,
- food allergy,
- copy of the first and second pages of the document suitable for identification and of the travel document.

Duration and means of processing:

The data are stored electronically and data processing lasts until the competent authority may check the fulfilment of the obligations specified by law.

Data transfer: to the Hungarian Tourism Agency, National Tourism Data Supply Centre.

6. MAGNETIC KEY CARD SYSTEM

Purpose of processing: facilitating the entry of guests into the rooms, checking the authorisations, property security.

Legal basis of processing: Article 6 (1) f) of the GDPR – legitimate interest;
Accordingly, an interest assessment test was performed.

Processed personal data:

- name (first and family name);
- room number;
- number of magnetic key card;
- day of arrival and departure.

Duration and means of processing: the data processing is performed electronically and lasts until the guest stays in the hotel.

7. GUEST BOOK

Purpose of processing:

- improving the quality of services at the Controller;
- accurate investigation of potential complaints, offering the possibility to the Controller to reply to the guest.

Legal basis of processing: pursuant to Article (6) (1) a) of the GDPR, the freely given consent of the Data Subject

Data processing is performed on the basis of the freely given, informed consent of the Data Subject.

The consent is given by the Data Subject by providing the concerned data freely, by entering the data in the guest book.

Processed personal data:

- name of the data subject;
- opinion of the data subject;
- email address.

Duration and means of processing: the processing of the provided data is performed in hard copy (Guest Book) and electronically (potential complaints) until the data subject withdraws the consent, or in case of complaint, until the investigation is performed and the reply is given.

8. DATA PROCESSING IN RELATION TO INVOICING

Purpose of processing: invoicing of the services provided by the Controller, compliance with the invoicing obligation, performance of the payment transaction.

Legal basis of processing: Article 6 (1) c) of the GDPR and Section 169 e) of Act CXXVII of 2007 on value added tax.

Processed personal data:

- name (first name and family name)
- residential address
- email address

Duration and means of processing:

Data storage is performed electronically. The deadline of erasing data is 8 years pursuant to Section 169 of Act C of 2000 on Accounting.

Data transfer: to OTP, for performing the payment transaction.

9. ELECTRONIC MONITORING SYSTEM

Purpose of processing: cameras are located in the area of the hotel operated by the Controller for safeguarding the life, physical integrity and property of the Guests, and signs draw the attention of the data subjects to this fact. Pertaining to the operation of the monitoring system, the Controller provides a separate notice to the Data Subjects.

Legal basis of processing: Article 6 (1) f) of the GDPR – legitimate interest;
Accordingly, an interest assessment test was performed.

Processed personal data:

- Data Subjects: employees, guests, visitors
- processed data: the images, bodies and movements of the Data Subjects.

Duration and means of processing:

- the recordings are stored by the Controller for 72 hours.
- the recordings are stored by the camera system on a server.

Data transfer:

The recorded images are transferred if, on the basis of the recordings, the commitment of a crime (offense) seems to be likely. In such case, the recordings are transferred to the investigating authority, or, if other legal proceedings need to be initiated on the basis of the recordings, to the competent court or authority.

10. DATA PROCESSING

Hotelsystem Kft.	Registered seat: 4400 Nyíregyháza, Őz köz 37. Fsz. 1. ajtó Company reg.no.: 15-09-076644 VAT number: 22992011-2-15	Hotel administration system required for compliance with the legal obligation specified in Section 9/H of Act CLVI of 2016 on state functions pertaining to the development of tourism regions
Accounting firm	Registered seat:	

	Company reg.no.: VAT number:	Accounting activity (for compliance with taxation and accounting obligations)
Temarketinged Kft.	Registered seat: 4024 Debrecen, Wesselényi utca 1. VAT number: 32037704209 Company reg.no.: 09-09-034197	Providing website development and maintenance services
KBOSS.hu Kft.	Registered seat: 1031 Budapest, Záhony utca 7. Company reg.no.: 01-09-303201 VAT number: 13421739-2-41	Data required for issuing the invoice for the Data Subjects are transferred to Számlázz.hu, which are then stored by the processor in an online system, and the processor issues invoices with the data content provided by the controller on behalf of the controller
HOSTINGER, UAB	Registered seat: Jonavos str. 60C, 44192 Kaunas, Lithuania	Web hosting provider of interhotel.hu website
Cívis Elektronik Plusz Kft	Registered seat: 4032 Debrecen Derék utca 124 2/7 VAT number: 25917192-2-09	Company performing the maintenance of the IT system, camera and alarm system of Inter Hotel

11. Data Subjects' Rights

Rights of data subjects: the data subject

a) may request information on the processing of his/her personal data, and access to such data,
b) may request the rectification of the data,
c) may request the erasure of the data,
d) may request the restriction of the processing of the personal data,

e) may object to the processing of the personal data,
f) may exercise his/her right to data portability,
g) and may exercise his/her right to remedy.

The Data Subject may file a complaint to the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter: NAIH) in accordance with the requirements set out at the end of this notice, or may turn to the competent court.

0. Data Subjects' Rights pertaining to Processing

The Controller guarantees that the data subjects' rights can be exercised as follows.

The Controller offers the possibility to the data subject to file his/her request pertaining to the exercising of the data subjects' rights in any manner specified below, to the contact details contained herein: (i) by mail, (ii) by email, (iii) by phone.

Phone: +36209182677
Email: inter.deversor@gmail.com
Mailing address: 4032 Debrecen, Gyimes utca 4.

The Controller responds to requests from the data subject without undue delay and at the latest within 30 days following the receipt of the request, and informs the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The Controller shall make a decision on rejecting the request within the same deadline, and shall notify the data subject on the rejection, on the reasons thereof and on the related remedy options.

As a rule, the Controller shall fulfil the data subject's request by email, unless otherwise requested by the data subject. At the data subject's request, information may only be provided by phone if the data subject has confirmed his/her identity. The Controller does not use the data subjects' mailing address or phone number for any other purpose.

For the fulfilment of the data subjects' requests detailed below, the Controller does not charge any fee or cost. However, where the Controller receives unfounded, excessive requests from a data subject repeatedly for the same set of data within one year following the previous already fulfilled request, the Controller reserves the right to charge a reasonable fee for the fulfilment of the request proportionately with the work done for fulfilling the request, or to reject any measures on the basis of the request at its discretion, with proper explanation.

- **Right to information and access**

At the data subject's request, the Controller shall provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language on the following:

- whether or not personal data concerning him or her are being processed by the Controller;
- the name and contact details of the Controller;
- his/her personal data processed by the Controller and information concerning the source of such data;
- the purpose of processing the personal data and the legal basis of processing;
- the duration of processing;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed;
- the data subject's rights;
- the circumstances, effects of a potential data breach and the measures taken for eliminating the breach.

- **Right to rectification**

At the data subject's request, the Controller rectifies the inaccurate personal data concerning the data subject.
The Controller shall inform all recipients on the rectification to whom the personal data have been disclosed, except where this proves to be impossible or would involve a disproportionate effort. At the data subject's request, the Controller informs the data subject on such recipients.

- **Right to erasure ("right to be forgotten")**

At the data subject's request, the Controller shall erase the personal data concerning him or her where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject objects to the processing;
- the personal data have been unlawfully processed by the Controller;
- the personal data have to be erased for compliance with a legal obligation in Union or Hungarian law to which the Controller is subject.

The Controller shall inform all recipients on the erasure to whom the personal data have been disclosed, except where this proves to be impossible or would involve a disproportionate effort. At the data subject's request, the Controller informs the data subject on such recipients.

- **Right to restriction of processing**

At the data subject's request, the Controller shall restrict processing where one of the following grounds applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the Controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.

The Controller shall inform all recipients on the restriction to whom the personal data have been disclosed, except where this proves to be impossible or would involve a disproportionate effort. At the data subject's request, the Controller informs the data subject on such recipients.

- **Right to data portability**

At the data subject's request, the Controller provides him/her the personal data concerning the data subject, which he or she has provided to the Controller. Furthermore, the Controller agrees that the data subject has the right to transmit those data to another controller without hindrance from the Controller.

- **Right to remedy**

Pursuant to the relevant legal regulations, where the data subject has reasons to consider that the Controller violated his/her right to the protection of personal data during processing, he/she may opt for remedy at the competent authorities, i.e. may file a complaint to NAIH (address: H-1055 Budapest, Falk Miksa utca 9-11.; mailing address: 1363 Budapest, Pf. 9.; website: www.naih.hu; email address: ugyfelszolgalat@naih.hu; phone number: +36-1/391-1400), or may turn to the competent court.

The Controller undertakes to cooperate with the competent court or NAIH in such procedures, and to provide the data pertaining to processing to the competent court or NAIH.

Furthermore, the Controller covenants to reimburse any and all damages caused by the unlawful processing of the data subject's personal data or by breaching the requirements of data security. In case of violating the data subject's privacy rights, the data subject may claim grievance fee. The Controller shall not be held responsible if the damage was caused by unavoidable causes beyond the scope of processing, or if the damage or the grievance caused by the violation of the privacy right arose due to the data subject's wilful or gross negligence.

0. DATA SECURITY MEASURES

The Controller ensures the security of data. The Controller has taken all technical and organisational measures and developed its rules of procedure to ensure the protection of the recorded, stored and processed data, and to prevent the destruction, unauthorised use and unauthorised alteration of such data. Furthermore, it draws the attention of the third parties to whom the data of the data subject have been disclosed that they are also obliged to comply with the requirements of data security.

The Controller ensures that the processed data cannot be accessed, disclosed, transferred, modified or erased by unauthorised persons.

The Controller shall do its best to prevent damages and destruction of the data. The Controller also requires its employees and partners participating in the data processing activities, as well as the processors acting on behalf of the Controller to comply with the aforesaid obligation.

0. HANDLING DATA BREACHES

If the Controller notices any event or act leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the Controller (hereinafter jointly referred to as: data breach), it shall act in accordance with Articles 33-34 of the GDPR, report the data breach to the competent data protection authority (hereinafter: NAIH), and inform the data subject or data subjects on the data breach, if it is likely to result in a high risk to the rights and freedoms of natural persons.

The person who notices a data breach as specified above in relation to the personal data transmitted, stored or otherwise processed by the Controller may notify the Controller at the following contact details:
By phone: +36209182677
By email: inter.deversor@gmail.com

The person submitting the report shall indicate the following in addition to the subject of the data breach:

- the name of the reporting person;
- the contact details of the reporting person: phone number and/or email address;
- whether the data breach affects the software, if yes, which part or service is affected.

The Controller shall investigate the breach within 1 business day at the latest, or if the data breach is considered serious, without delay, and – if needed – requests further data from the reporting person. The Controller provides data to NAIH within 72 hours following the reporting of the data breach.

The provided data shall include the following:

- nature of the data breach, including the categories and estimated number of data subjects, and the categories and estimated number of data affected by the data breach;
- the name and contact details of the person providing further information;
- the likely consequences arising from the data breach;
- the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where the data breach requires further investigation, the Controller shall take the necessary measures to involve the proper experts and to assess the actual and potential effects of the data breach. The experts shall prepare a report. The report shall contain proposals concerning the security measures required for eliminating the breach.

The Controller shall make decisions on taking the measures.

The Controller shall communicate to the data subject the personal data breach without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

In the communication, the Controller shall provide information in a clear and plain language on the nature of the data breach, including the following:

- name and contact details of the person providing further information;
- the likely consequences arising from the data breach;
- the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Controller shall not inform the data subjects if:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- the communication would involve disproportionate effort, i.e. there is such a large number of data subjects that the Controller could only inform them by making disproportionate efforts. In such case, the Controller takes measures to disclose the proper information.

0. Registration of Personal Data Breaches

The Controller shall keep records of the data breaches.

The records shall contain:

- the scope of the affected personal data,
- the scope and number of persons affected by the data breach,
- the date of the data breach,
- the circumstances and effects of the data breach,
- the measures taken for eliminating the data breach,
- other data specified by the legal regulation requiring the processing.

The data pertaining to the data breach contained in the records shall be kept by the Controller for 5 years in case of breaches affecting personal data, and for 20 years in case of breaches affecting special data.

0. Right to Remedy

The Controller may be contacted at the contact details set out herein in relation to any question or remark pertaining to processing.
Requests for remedy or complaints may be filed to the Hungarian National Authority for Data Protection and Freedom of Information:

Name: Hungarian National Authority for Data Protection and Freedom of Information
Registered seat: H-1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1363 Budapest, Pf. 9.
Phone: +36-1-391-1400
Fax: +36-1-391-1410
Website: www.naih.hu
Email: ugyfelszolgalat@naih.hu

In case of violating the data subject's rights, the data subject may turn to court against the Controller. The court gives priority to such cases. The Controller shall prove that the processing complies with the law. The lawsuit shall be assessed by the regional court. At the discretion of the plaintiff, i.e. the data subject, the lawsuit may be initiated before the court operating at the data subject's place of residence or place of stay.

The Controller undertakes to cooperate with the competent court or NAIH in such procedures, and to provide the data pertaining to processing to the competent court or NAIH.

Furthermore, the Controller covenants to reimburse any and all damages caused by the unlawful processing of the data subject's personal data or by breaching the requirements of data security. In case of violating the data subject's privacy rights, the data subject may claim grievance fee. The Controller shall not be held responsible if the damage was caused by unavoidable causes beyond the scope of processing, or if the damage or the grievance caused by the violation of the privacy right arose due to the data subject's wilful or gross negligence.

The Controller reserves the right to amend this notice anytime.