Case number: NAIH/2020/2305/
In charge: [redacted]

Re: Decision

DECISION

The **Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information,** hereinafter: Authority) brings the following decisions in its data protection procedure launched ex officio against [redacted] (registered office: [redacted] hereinafter: Obligee), in which the Authority investigated the compliance by the Obligee with the provisions of the General Data Protection Regulation (hereinafter: GDPR):

I. The Authority **establishes** that the Obligee acted unlawfully and infringed the provisions of GDPR, when it

I.1. failed to make the information on its data processing easily accessible, thereby infringing Article 12(1) of GDPR;
I.2. failed to take action within a month from the receipt of the access request, thereby infringing Article 12(3) of GDPR;
I.3. failed to provide full information upon the access request, thereby infringing Article 15(1) of GDPR;
I.4. made a photo recording of the identification document of the person making use of its accommodation service, thereby infringing Article 5(1)(c) of GDPR;
I.5. uploaded the photo made of the identification document to the Obligee's WhatsApp group, thereby infringing Article 6(1) of GDPR.

II. The Authority **orders** the Obligee to

II.1. make its information on data processing easily accessible on its website on the landing page, as well as in the course of reservation;
II.2. provide the Customer information on the processing of his personal data, covering all the aspects of data processing in accordance with Article 15(1) of GDPR within 30 days from this decision becoming final.
II.3. refrain from making photo recording of identification documents of its guests.

IV. The Authority imposes

a data protection fine of
HUF 360,000, that is, three hundred and sixty-thousand forints

because of the unlawful processing of data, payable within 30 days from this decision becoming final.

* * *

Obligee shall notify the Authority of the implementation of the measures set forth in Section II within 8 days from taking them, also enclosing the substantiating evidence.

The fine is to be paid to the targeted forint account of the Authority for the collection of centralised revenues (10032000-01040425-00000000 Centralised collection account IBAN: HU83 1003 2000 0104 0425 0000 0000). When transferring the amount, reference is to be made to this number: NAIH/2020/2305. BÍRS.

In the event that the Obligee fails to meet its obligation to pay the fine when due, it shall pay a penalty for delay. The rate of the penalty for delay is the legal interest rate corresponding to the central bank base rate quoted on the first day of the calendar half year affected by the delay.

In the event of a failure to meet the obligations according to Section II or the non-payment of the fine and a penalty for delay according to Section III, the Authority orders the execution of its decision.

There is no legal remedy against this decision through the administrative route, but it can be attacked in an administrative lawsuit through a petition addressed to the Fővárosi Törvényszék (Budapest Tribunal) within 30 days from its communication. The petition is to be submitted to the Authority electronically,[1] and the Authority will forward it together with the documents of the case to the Tribunal. For those who are not fully personally exempted from duty, the duty of an administrative lawsuit is HUF 30,000; the lawsuit is subject to the right of prenotation of duties. Legal representation is mandatory in a procedure in front of the Budapest Tribunal.

JUSTIFICATION

I. The course of the procedure

Based on the Client's complaint, the Berlin Data Protection Authority initiated a procedure to establishment the lead supervisory authority and the other authorities concerned in accordance with Article 56 of GDPR through the IMI system under case number 63831 on 29 March 2019. The Client was unable to name the controller, it could pinpoint only its website, which is [redacted] (hereinafter: website).

Based on the website, the person of the controller could not be established as it did not display the name of the company operating the website, only its address ([redacted]) and the name of the managing director. According to public company information, no company providing accommodation services was registered to the address indicated in the website, but based on public company information, the Authority found a company called [redacted], whose registered offices are located at [redacted]

In view of the above, it was probable that the central operations of the presumed controller was in Hungary, so the Authority stated in the procedure according to Article 56 of GDPR that in its view the Authority is the lead supervisory authority in this case. After this, the Berlin Data Protection Authority sent the detailed complaint of the Client, his name and access data to the Authority on 31 May 2019.

The Authority launched an investigative procedure under case No. NAIH/2019/3239, of which it informed [redacted] at the address of [redacted] in a letter dated 27 June 2019 and called upon the company to answer the questions of the Authority with a view to clarifying the facts of the case. [redacted] received the Authority's letter on 8 July 2019. The Authority sent its letter also to the e-mail address displayed in the website [redacted] as well as to the mailing address indicated in the website: [redacted] The Authority's letter sent to [redacted] was answered by [redacted] which had the same registered address as according to their statement, the Obligee was the controller in the case. The Obligee's statement was received by the Authority on 25 July 2019.

Simultaneously with contacting the undertaking presumed to be the controller, the Authority also contacted the Client, asking him to make his personal identification data and address available to the Authority and requested

[1] An administrative lawsuit can be initiated by using the form NAIH_K01: NAIH_K01 űrlap (16.09.2019) The form can be filled in using the general form fill-in program (ÁNYK program).

him that in the event that he received an answer to his access request from the controller since lodging the complaint with the Berlin Data Protection Authority, he should send it to the Authority. The Client's answer was received by the Authority on 31 July 2019.

In view of the fact that the Obligee failed to answer all the questions of the Authority the first time with respect to the processing of the Client's personal data, the Authority contacted the Obligee again on 12 December 2019. The Authority received the Obligee's statement on 30 December 2019 and it submitted additional evidence on 29 January 2020.

On 16 January 2020, the Authority informed both the Client and the Berlin Data Protection Authority that the procedure was still in progress.

On 4 March 2020, the Authority launched its data protection procedure ex officio in the case pursuant to Section 55(1)(ab) and Section 60(3)(b) of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act), of which it informed the Obligee on the same day, and called upon it to make statements in order to clarify the facts of the case.

The Obligee's statement was received by the Authority by e-mail on 26 March 2020 and on 31 March by mail.

Upon its request, the Authority informed the Berlin Data Protection Authority that the investigative procedure in the case was closed and the data protection procedure was launched on 31 March 2020.

II. The facts of the case

In his complaint lodged with the Berlin Data Protection Authority, the Client (his reservation numbers: 1681390; 2635357; 5376220) presented that he reserved accommodation through the website where he did not find information on data processing, so he was unable to study the Privacy Policy in advance.

When arriving at the accommodation on 3 November 2018, he and his companion had to fill in a form required for registration where they had to state their names, addresses, birth dates, the number of their identification documents, their e-mail addresses and phone numbers. After this, the employee of the landlord asked for the Client's identification document in order to make a photo of it using his smart phone. The Client first refused to do so, when the employee of the landlord informed him that in the absence of this, they will not be able to register and occupy the accommodation, so finally the photo was made of the identification document of his companion, which the employee uploaded to a group chat in WhatsApp.

On 7 November 2018, the Client submitted a request to access from the e-mail address [redacted] to the Obligee, in which he requested information on all his personal data processed by the Obligee on the basis of Article 15 of the General Data Protection Regulation (hereinafter: GDPR)[2]. He also requested information on the forwarding of the data through WhatsApp, as well as the data storage in that application. On 8 November 2018, he received an answer from the e-mail address [redacted] informing him that his request was forwarded to the managing director, from whom he will get an answer within a few days. The Client did not receive any answer to his access request by 5 December 2018 when he sent his submission to the Berlin Data Protection Authority.

[2]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).

The Client complained that no information on data processing was available in the website and that he did not receive an answer to his access request sent to the contact e-mail address of the landlord. He also objected to the fact that the employee of the landlord wished to make a photo of his identification document and that the employee of the landlord uploaded the photo of the identification document of his companion to the Obligee's WhatsApp group, which includes only a few employees of the Obligee and is used for sharing information in connection with the individual apartments rapidly.

Upon the first call of the Authority, the Obligee failed to give concrete answers concerning the Client, except for the screenshot of the registry concerning the Complainant and generally informed the Authority on data processing.

According to the Obligee's statement, guests are informed of its Privacy Policy available in the website [redacted] (hereinafter: Privacy Policy).

In the course of making the reservation, guests have to indicate that they accept the provisions of the Privacy Policy. The Obligee stated that the Privacy Policy is available to the guests in English and in Hungarian in every apartment.

In relation to the access request, the Obligee informed the Authority that it answered the request on 19 July 2019; the answer was delayed because of an administrative mistake. The copy of the answer was sent by the Obligee to the Authority.

The Obligee informed the Authority through his authorised representative that it only processes the name of the Client on the accounting voucher issued for him, the copy of which was sent to the Authority. The legal basis for processing the Client's name in the accounting voucher was Article 6(1)(c) of GDPR as Section 169(2) of Act C of 2000 on Accounting (hereinafter: Accounting Act) requires the Obligee to keep accounting vouchers for eight years. The purpose of data processing, i.e. keeping the accounting voucher, is to meet accounting obligations.

The Obligee supplemented its earlier statement stating that the delay in answering the access request of the Client took place because the employee handling incoming e-mails did not pay attention to it and he did not attach any significance to it. When GDPR became applicable, the Obligee developed an internal data processing protocol, provided training for the employees, still the omission took place on the part of the employees.

The Obligee deleted the photo made of the identification document of the Client's companion from the WhatsApp group; to substantiate this, it enclosed the screenshot of the chat in the WhatsApp group.

III. Applicable legal regulations

Pursuant to Article 2(1) of GDPR, GDPR is to be applied to data processing according to this case.

The provisions of GDPR relevant to this case are the following:

GDPT Article 5(1)(c): *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation").*

GDPR Article 12(1): *The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including where appropriate by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.*

GDPR Article 12(3): *The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means, where possible, unless otherwise requested by the data subject.*

GDPR Article 15(1): *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and where that is the case, access to the personal data and the following information:*
a) the purposes of data processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient, to whom the personal data have been or will be disclosed, in particular, recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller, rectification or erasure of personal data or restriction of processing of personal data concerning the data subject, or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4), and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Accounting Act Section 169(2): *The accounting vouchers (including general ledger accounts, analytical and detailed records) directly or indirectly substantiating bookkeeping shall be kept in a legible form, enabling their search based on references in the bookkeeping notes for at least eight years.*

GDPR Article 58(2)(b), (c) and (i): *Each supervisory authority shall have all of the following corrective powers:*
b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this regulation;
c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this regulation;
i) to impose an administrative fine pursuant to Article 83, in addition to or instead of measures referred to in this paragraph depending on the circumstances of each individual case.

GDPR Article 77(1): *Without prejudice to any other administrative or judicial remedy. every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*

GDPR Article 83(1)-(2) and (5)(a)-(b): (1) *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this article in respect of infringements of this Regulation referred to in paragraphs (4), (5) and (6) shall in each individual case be effective, proportionate and dissuasive.*

(2) Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in point (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them;
b) the intentional or negligent character of the infringement;
c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
e) any relevant previous infringements by the controller or the processor;
f) the degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
g) the categories of personal data affected by the infringement;
h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent the controller or processor notify the infringement;
i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject matter compliance with those measures;
j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42, and
k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement-

(5) Infringement of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to EUR 20,000,000, or in the case of an undertaking up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
b) the data subjects' rights pursuant to Articles 12 to 22.

Privacy Act Section 2(2): *Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: "General Data Protection Regulation") shall apply to the processing of personal data falling within the scope of the General Data Protection Regulation, with the additional rules laid down in Chapters III to V and VI/A, as well as in Section 3, points 3, 4, 6, 11, 12, 13, 16, 17, 21, 23 to 24, in Section 4 (5), Section 5 (3) to (5), (7) and (8), Section 13 (2), Section 23, Section 25, Section 25/G (3), (4) and (6), Section 25/H (2), Section 25/M (2), Section 25/N, Section 51/A (1), Sections 52 to 54, Section 55 (1) to (2), Sections 56 to 60, Section 60/A (1) to (3) and (6), Section 61 (1) a) and c), Section 61 (2) and (3), (4) b) and (6) to (10), sections 62 to 71, section 72, Section 75 (1) to (5), Section 75/A and Annex 1.*

Pursuant to Section 60(1) of the Privacy Act, *to ensure that the right to the protection of personal data is enforced, the Authority may commence an administrative procedure for data protection ex officio. The rules of Act CL of 2016 on General Administrative Procedures (hereinafter: Administrative Procedures Act) shall be applied to the data protection procedure of the Authority with the additions specified in the Privacy Act and the differences according to the General Data Protection Regulation.*

Privacy Act Section 75/A: *The Authority shall exercise its powers specified in Article 83(2) to (6) of the General Data Protection Regulation according to the principle of proportionality, in particular by primarily issuing, in compliance with Article 58 of the General Data Protection Regulation, a warning to the controller or processor for the purpose of remedying the infringement when the provisions laid down by law or a binding legal act of the European Union on the processing of personal data are first infringed.*

The rules of Act CL of 2016 on General Administrative Procedures (hereinafter: Administrative Procedures Act) shall apply to the data protection procedure of the Authority with the additions specified in the Privacy Act and the differences according to the General Data Protection Regulation.

IV. The decision:

IV.1. Access to information

Article 12 of GDPR specifies the formal requirements which controllers must take into account when enabling the exercise of the rights of data subjects, including the provision of information in advance to data subjects. Accordingly, controllers must provide all information concerning the processing of personal data in a concise, transparent, intelligible and easily accessible form. This is supplemented by Article 13(1) of GDPR with the requirement that where personal data relating to a data subject are collected from the data subject, the controller shall inform the data subject of the circumstances of data processing at the time when the personal data are obtained.

According to the statement of the Client, he found no information concerning the processing of personal data on the website at the time of lodging his complaint.

Prior to launching the investigative procedure, the Authority checked the website of the Obligee where no page was found that would have contained the Privacy Policy or would have directed the viewer to it (screenshot: 2 April 2019, 18 June 2019).

In November 2019, the Authority examined the website of the Obligee again where there was a page entitled Policies; however under the Privacy Policy tab only some Latin sample text was found which was used for editing the website and not the Privacy Policy.

In November 2019 and also at the time of bringing this decision, the link pointing to the Privacy Policy became accessible when the guest or the future guest began reservation and chose the date of stay. In relation to the selected date, the website lists all the apartments, namely more than a hundred, that can be rented from the Obligee, irrespective of whether or not they are available and the link to the Privacy Policy appears first at the end of this list; once the apartment is selected, it becomes accessible also in the right band of the website. It is, however, not possible to click on the link, i.e. the Privacy Policy can be read only if the link is copied into a new browser window.

As the last step of reservation, the future guests must provide their personal data and have to tick a box stating that they have read and accepted the terms and conditions of use and the provisions of the Privacy Policy[3], but a clickable link pointing to the Privacy Policy is not available here either (screenshots: 27. 11. 2019.), i.e. the Privacy Policy is accessible only from the link placed at the bottom of the page or through the link located in the side band of the website, which cannot be clicked.

[3] "I have read and accepted the Terms and conditions and Privacy Policy."

Based on the above, the Authority established that the Obligee infringed Article 12(1) of GDPR as it provides information to the data subject on the processing of their personal data in a form that is not easily accessible.

IV.2. Meeting the Client's access request

The Client submitted a request for the exercise of his right of access to the Obligee on 7 November 2018, which the Obligee answered in merit only on 19 July 2019 after being called upon to do so by the Client on 11 July 2019, and after the notification of the Authority on launching the investigative procedure.

Hence, the Authority establishes that the Obligee infringed Article 12(3) of GDPR with respect to the Client's access request, as it informed the Client on the processing of his personal data only after the one-month period specified in GDPR.

In view of the fact that the Obligee took action to remedy the infringement only after learning of the procedure by the Authority, i.e. the Client did not receive any information on the processing of his personal data for more than seven months from the submission of his access request, the Authority also establishes the infringement of the Client's right to access according to Article 15 of GDPR.

IV.3. The adequacy of the answer given to the Client's access request

The Client requested information on all his personal data processed by the Obligee taking into account all the circumstances of Article 15 of GDPR.

As against this, Obligee only informed the Client that it was processing his personal data in accordance with the Accounting Act. It is the position of the Authority that the Client cannot be expected to know the provisions of the Accounting Act.

In its answer, the Obligee did not tell what personal data were processed for what purpose and for how long, nor was the Client informed on whether or not the Obligee communicated his personal data to third persons. Moreover, it failed to inform the Client on the rights due to him in relation to data processing (GDPR Article 15(1)(e)), or of the fact that he may turn to the supervisory authority with his complaint (GDPR Article 15(1)(f)).

The Privacy Policy attached to the reply provides general information on the processing of data, i.e. it serves to meet the general obligation to provide information according to Article 13 of GDPR. As against this, in the case of requests aimed at exercising the right to access according to Article 15 of GDPR, the information to be provided must be concrete and cover the actual processing implemented in relation to the given data subject, because short of this the data subject's right to check the lawfulness of the processing of his personal data is breached.

Providing information by way of the Privacy Policy is inadequate in the case of an access request, because the Privacy Policy provides information on all data processing, even if it is contingent, and not all of these processing acts are relevant in relation to processing the data of the particular data subject. It is the obligation of the controller to assess how it actually processes the personal data of a given data subject and it is of this that it must provide information based on an access request according to Article 15 of GDPR.

The part of the request, which applies to the uploading of personal data to WhatsApp and the storage of the data there cannot be regarded as a request to exercise the right of access as the photo was made of the

document not of the client, but of his companion. The Client did not discuss this in his request sent to the Obligee, it is revealed only from the complaint lodged with the Berlin Data Protection Authority. It follows that these questions of the Client can only be regarded as requesting general information and not as an access request, as the essence of the right to access is that the data subject should get information on the processing of his personal data and not those of third persons.

Based on the above, the Authority establishes that the Obligee infringed the Client's right to access according to Article 15(1) of GDPR, when despite the Client's express request formulated in the access request, it failed to provide information on all the circumstances specified in Article 15(1) of GDPR in relation to the processing of the personal data.

IV.4. The lawfulness of making a photo of the document of the Client's companion and its uploading to the WhatsApp group

In every case, the processing of personal data is an intervention into the privacy of the data subjects. According recital (3) of GDPR, personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. Consequently, controllers must consider in the first place whether achieving their desired purpose requires the processing of the personal data. If the purpose can only be fulfilled by processing the personal data, its process should be developed on the basis of the principle of data minimisation, so that as few personal data should be processed as possible for the shortest possible period.

The Obligee's employee made a copy of the document of the Client's companion in order to see whether the personal data provided upon registration were true.

Based on its statement, the Obligee was fully aware that to check whether the personal data provided by its guests are true, it is enough to have the identification documents presented, and it is not necessary to make copies of the documents of guests and to store them.

Based on the above, the Authority established that the Obligee infringed the principle of data minimisation according to Article 5(1)(c) of GDPR by making a photo of the identification document of the Client's companion with a view to checking the correctness of the data provided upon registration.

The employee of the Obligee did not have any of the legal basis listed in Article 6(1) of GDPR for uploading the photo made of the identification document to the WhatsApp group because the data subject did not grant his consent for that, it was not necessary for performing a contract, no legal regulation required him to do so, nor did he have any legitimate interest in doing so that could override the interests and fundamental rights and freedoms of the data subject. The application of the legal basis according to Article 6(1)(d) and (e) of GDPR is, by definition, excluded.

It follows that the Authority established that the employee of the Obligee provided access to the personal data of the Client's companion to the other employees of the Obligee unlawfully without any legal basis, thereby infringing Article 6(1) of GDPR.

IV.6. Legal consequences

IV.6.1. In its data protection procedure launched ex officio, the Authority established based on Article 58(2)(b) of GDPR that the Obligee infringed Article 5(1)(c), Article 6(1), Article 12(1) and (3), and Article 15(1) of GDPR.

IV.6.2. The Authority orders the Obligee to make his Privacy Policy available on the landing page of his website, as well as in the course of reservation, bearing in mind Section IV.1. of the justification of the decision.

IV.6.3. The Authority orders the Obligee to provide information on the processing of his personal data extending to all aspects of processing to the Client, taking Section IV.3. of the justification of this decision into account.

IV.6.4. The Authority orders the Obligee to refrain from making photo recording of identification documents of its guests, bearing in mind Section IV.1. of the justification of the decision.

IV.6.5. The Authority examined whether imposing a data protection fine against the Obligee was warranted.

In this respect, the Authority considered all the circumstances of the case based on Article 83(2) of GDPR and Section 75/A of the Privacy Act. In view of the circumstances of the case, the Authority established that in the case of the infringement exposed in the course of this procedure, a reprimand is not a proportionate sanction of restraining force, hence it is necessary to impose the fine.

First and foremost, the Authority considered that the infringements by the Obligee qualify as infringements in the higher fine category according to Article 83(5)(b) of GDPR as it involved the infringement of the principles of processing and the violation of the rights of the data subject.

In imposing the fine, the Authority assessed the following circumstances as factors increasing the amount of the fine:

- the difficult access to the Privacy Policy as infringement can be regarded as lasting, as it existed for at least a year. In addition, this affected not only the Complainant, but every natural person who reserved accommodation through the website of the Obligee. According to the statement of the Obligee, 829 reservations were made through the website between 25 May 2018 and March 2020 [GDPR Article 83(2)(a)];

- in the course of the processing under review, the Obligee infringed several provisions of GDPR [GDPR Article 83(2)(a)];

- the Obligee's employee would have prevented the Client and his companion from occupying the accommodation earlier reserved and paid for by them, had the Client's companion not allowed him to make a photo of his identification document, i.e. the Client and his companion would have suffered damage, had they not given permission for the unlawful processing of their data [GDPR Article 83(2)(a)];

- Obligee failed to act sufficiently circumspectly in preparing its answer to the access request of the Client and failed to inform the Client of all the circumstances of processing according to Article 15(1) of GDPR even after learning of the investigative procedure, which was the antecedent of this procedure of the Authority [GDPR Article 83(2)(k)];

In the course of imposing the fine, the Authority assessed the following circumstances as factors reducing the amount of the fine:

- the infringements related to the exercise of the Client's right of access affected him alone and according to the Obligee's statement, other than that of the Client, it did not receive any request for the exercise of rights from data subjects since the entry into force of GDPR [GDPR Article 83(2)(a)];

- it was a circumstance indicative of negligence that human failure caused the non-fulfilment of the Client's access request and making the photo of the identification document of the Client's companion was also a result of an employee's error [GDPR Article 83(2)(b)];

- having learned of its failure, the Obligee attempted to fulfil the Complainant's access request [GDPR Article 83(2)(c)];

- this was the first time that the Obligee infringed the provisions of GDPR, earlier it did not commit relevant infringements, which is a substantial mitigating circumstance, which should be taken into account also based on Section 75/A of the Privacy Act [GDPR Article 83(2)(e)];

- the main activity of the Obligee is the provision of accommodation services made use of largely by tourists. The pandemic caused by the COVID-19 virus caused substantial loss of revenue in the second quarter of 2020 in tourism, thus presumably also at the Obligee [GDPR Article 83(2)(k)].

In addition, the Authority took into account that

- the Obligee met its obligation to cooperate with the Authority [GDPR Article 83(2)(f)];
- the established data protection infringements do not affect the special categories of personal data [GDPR Article 83(2)(g)];
- According to the Obligee's 2018 annual report, its pre-tax profits amounted to HUF 61,149,000, while in the year in question it was HUF 55,456,000. The amount of the data protection fine imposed amounts to 0.49% of the Obligee's pre-tax profits [GDPR Article 83(5)];

In imposing the fine, the Authority did not regard the circumstances according to Article 83(2)(d), (h), (i) and (j) of GDPR as relevant for the concrete case.

The Authority determined the amount of the fine acting within its powers of consideration based on legal regulation.

Based on the above, the Authority decided as presented in the operative part.

V. Miscellaneous issues

The powers of the Authority are set forth in Section 38(2) and (2a) of the Privacy Act, its competence extends to the entire territory of the country.

These decisions are based on Sections 80-81 of the General Administrative Procedures Act and Section 61(1) of the Privacy Act. The decision and the warrant become final upon their communication pursuant to Section 82(1) of the General Administrative Procedures Act. Pursuant to Sections 112 and Section 114(1) of the General Administrative Procedures Act, legal remedy against the decision may be obtained through administrative litigation.

***

The rules of administrative litigation are specified in Act I of 2017 on the Code of Administrative Litigation (hereinafter: Administrative Litigation Act). Pursuant to Section 13(3)(a)(aa) of the Administrative Litigation Act, a tribunal has competence for the administrative litigation against the decision of the Authority and the Budapest Tribunal has exclusive competence with regard to this litigation. Pursuant to Section 27(1)(b) of the Administrative Litigation Act legal representation is mandatory in administrative litigations under the

competence of a tribunal. Pursuant to Section 39(6) of the Administrative Litigation Act, the submission of a petition has no deferring effect on the administrative act entering into force.

Pursuant to Section 9(1)b) of Act CCXII of 2015 on the General Rules for Electronic Administration and Trust Services to be applied according to Section 29(1) of the Administrative Litigation Act and, in view of this, Section 604 of the Civil Procedures Act, the legal representative of the Client is subject to an obligation to maintain contact electronically.

Section 39(1) of the Administrative Litigation Act specifies the date and place of submitting the petition. The information on the possibility of a request for a hearing is based on Section 77(1)-(2) of the Administrative Litigation Act.

Section 45/A(1) of Act XCIII of 1990 on Duties (hereinafter: Duties Act) determines the magnitude of the duty for administrative litigation. Sections 59(1) and 62(1)(h) exempts the party initiating the procedure from the payment of the duty in advance.

Budapest, "16." December 2020

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG 1

Dr. Attila Péterfalvi
President
Honorary university professor