Case number: NAIH-406-21/2022.

(NAIH-7745/2021.)

Administrator: [...]

Subject: decision establishing a violation of law

H A T A R O Z A T

The National Data Protection and Freedom of Information Authority (hereinafter: Authority) is […]

Represented by the Law Firm (administrator lawyer: […]) […] (seat: […].; company registration number: [...];

your tax number; [...]; hereinafter: the online store operated by […]

data management, including generally ensuring the right of deletion of the data subjects and [...] (e-mail

it's title: […]; hereinafter: the applicant) to fulfill his request to delete his personal data a

on the protection of natural persons with regard to the management of personal data and that

on the free flow of such data and the repeal of Directive 95/46/EC

compliance with Regulation 2016/679 (EU) (hereinafter: General Data Protection Regulation).

in a data protection official procedure initiated ex officio for its investigation - in which the Authority is a client

provided legal status for the notifier as well - makes the following decisions:

1. The Authority determines that the Customer has violated it

- Paragraphs (1)-(2) of Article 13 of the General Data Protection Regulation;

- Article 6 (1) point a) of the General Data Protection Regulation;

- Article 7 (2) of the General Data Protection Regulation;

- Article 12 (4) of the General Data Protection Regulation;

- Article 17 (1) point b) of the General Data Protection Regulation;

- Article 12 (1) of the General Data Protection Regulation.

2. The Authority instructs the Client to

- provide appropriate, comprehensible and transparent information to all stakeholders

about data management and their circumstances;

- request the consent of the data subjects in an appropriate manner for data processing for marketing purposes,

respectively the already started, as well as

in the case of existing data management

confirmation of their consent, separate from the acceptance of the asf. In the absence of this

ensure the documented deletion of the personal data of the data subjects;

in progress

-

inform the notifier based on his request for the deletion of personal data

measures.

3. The Authority due to the violations established in point 1

HUF 500,000, i.e. five hundred thousand forints

data protection fine

obliges the Customer to pay.

4. The Authority also terminates the Customer's website, newsletter and SMS sender

seizure of databases operating behind its systems.

* * *

....

....

1055 Budapest

Falk Miksa utca 9-11

Phone: +36 1 391-1400

Fax: +36 1 391-1410

ugyfelszolgalat@naih.hu

www.naih.hu

Taking the measures prescribed in point 2 to the Customer upon receipt of this decision

must be in writing within 30 days - together with the submission of supporting evidence

- certify to the Authority.

The data protection fine shall be paid within 30 days of this decision becoming final

Authority's centralized revenue collection target settlement HUF account (10032000-01040425-

00000000 Centralized direct debit account IBAN: HU83 1003 2000 0104 0425 0000 0000)

must be paid. When transferring the amount, NAIH-406/2022. FINE. number must be referred to.

If the Customer does not comply with the obligation to pay the fine within the deadline, to the above account number

must pay a late fee. The amount of the late fee is the legal interest, which is a

it is the same as the central bank base rate valid on the first day of the calendar semester affected by the delay.

Non-fulfillment of the obligations according to point 2, as well as the data protection fine and late fee

in case of non-payment, the Authority orders the execution of the decision.

There is no place for administrative appeal against this decision, but from the announcement

within 30 days with a claim addressed to the Capital Tribunal in a public administrative case

can be attacked. The claim must be submitted to the Authority, electronically1, which is the case

forwards it to the court together with its documents. The request to hold the hearing must be indicated in the statement of claim

must For those who do not benefit from the full personal tax exemption, the administrative court fee

HUF 30,000, the lawsuit is subject to the right to record a material levy. In the proceedings before the Metropolitan Court, the

legal

representation is mandatory.

I N D O C O L A S

I. Procedure of the procedure

1. On February 16, 2021, the notifier filed a report with the Authority objecting that the

He asked in vain from the Customer operating the […] page on September 20, 2020 and November 22, 2020

deletion of personal data, the Customer's representative September 20, 2020 and November 2020

Contrary to the information you sent on the 30th - according to which it was deleted in addition to your purchase data

personal data - on January 28, 2021, he still received an electronic letter from the Customer.

2. In the case, point f) of Article 57 (1) of the General Data Protection Ordinance, respectively

CXII of 2011 on information self-determination and freedom of information. law (a

hereinafter: Infotv.) based on point a) of paragraph (3) of § 38. NAIH-2611/2021. case file number

an investigation procedure was initiated.

3. In the investigation procedure, the Customer stated that on September 7, 2020, the whistleblower

At 21:40 he ordered a birthday newspaper in the […] online store. When ordering, the general

contract conditions and several points of their customer card system were ticked and thus accepted

that information communication will take place to the specified e-mail address.

According to the Customer's statement, the internal newsletters are equipped with an immediate, automatic unsubscribe

link, but as the whistleblower indicated on September 20, 2020 that he does not wish to receive e-mails in the future

receive, deleted from their system.

According to the Customer's statement, in November 2020, the regular update of the newsletter,

due to its connection with the website, the database was resynchronized, which is why it was able to receive a new one

1 The NAIH_K01 form is used to initiate the administrative lawsuit: NAIH_K01 form (16.09.2019)

The form can be filled out using the general form filling program (ÁNYK program).

The form is available from the following link: https://www.naih.hu/kozig-hatarozat-birosagi-felulvizsgalata

inquiry by the notifier on November 20, 2020. In addition, the separate customer card database is one

fully automatic system from which you received a name day greeting.

According to the Customer's statement, on November 22, 2020 - and in the absence of an answer to this -

in their repeated letter of November 27, they also informed the whistleblower that from their newsletter system

and they deleted your personal data from all their similar lists, but they do not know all your personal data

delete, as they must store the basic data of the purchase. This information was confirmed by the Authority

information letter of November 30, 2020 available to the Customer.

According to the Customer's statement, the whistleblower on November 22, 2020 and again on November 27

after indicating that all your personal data, which is not required to be stored, was deleted, and a

his phone number was also transferred to the company phone number. Thus from the newsletter sender and customer card

database

their e-mail address and phone number were deleted from the delivery data.

Nevertheless, the screenshot attached to the letter filed with the Authority on May 21, 2021

according to the Customer's system, the telephone number and e-mail address of the notifier were still available.

4. The Authority, having reviewed what was written in the above answers of the Customer, dated June 16, 2021, NAIH-

2611-11/2021. with his letter with file number, Article 58 (2) paragraph b) of the General Data Protection Regulation

and c) and Infotv. On the basis of § 56, paragraph (1), he called on the Customer to

delete the e-mail address and telephone number of the notifier, given that they are to be managed by

Act C of 2000 on accounting (hereinafter: Act) and on general sales tax

CXXVII of 2007 Act (hereinafter referred to as the VAT Act) is not obliged, and its data management

it has no other legal basis.

At the same time, the Authority also notified the whistleblower about the Customer's notice, who on June 17, 2021.

informed the Authority that on March 9 and June 8, 2021, he received

an electronic letter from the Customer concerning the customer card, which, according to his opinion, indicates that

your personal data - your e-mail address and phone number - have not been deleted.

According to the receipt returned to the Authority, NAIH-2611 addressed to the Customer

11/2021. notice with file number was delivered to the Customer on June 21, 2021.

Infotv for the Customer. Pursuant to § 56, paragraph (2) - if you agree - immediately

he should have taken the necessary measures indicated in the notice, and he did

measures, or - in case of disagreement - his position from the receipt of the notice

would have been obliged to inform in writing, supported by documents, within thirty days

the Authority, which, however, did not take place, the Client did not respond to the Authority's letter.

Therefore, the Authority dated August 5, 2021, NAIH-2611-14/2021. with his letter with file number

points b) and c) of Article 58 (2) of the General Data Protection Regulation, as well as the Infotv. Section 56 (1)

repeatedly called on the Customer to delete the e-mail address of the notifier

and telephone number, given that the Szt. and VAT tv. is not obliged based on

and there is no other legal basis for data processing.

According to the receipt returned to the Authority, NAIH-2611-14/2021. case file number

notice was also delivered to the addressee on August 10, 2021. To the Customer

the Infotv. Pursuant to § 56, paragraph (2), it should have been done immediately if he agreed

should do that

and the done

measures, or - in case of disagreement - his position from the receipt of the notice

would have been obliged to inform in writing, supported by documents, within thirty days

the Authority, which, however, also did not take place, and the Customer repeatedly did not respond to

To the authority's letter.

On the basis of the above, since in accordance with the Authority's calls to remedy the infringement, no

took place, the Authority is Infotv. Section 55. (1) point a) subpoint b) and Infotv. Section 58 (2)

based on paragraph a) the investigation was closed and on October 14, 2021 ex officio data protection

initiated an official procedure for the exercise of the rights of the data subject according to the notification, and in general for

the cancellation

indicated in the notice is required

measures

repeated

4

concerning the fulfillment of rights. The period under review is from May 25, 2018 to the present data protection authority

it covered the period up to the date of initiation of the procedure.

The Authority is Infotv. In view of Section 71 (2) in this official data protection procedure

used by the preceding NAIH-2611/2021. lawfully during the investigation procedure initiated under No

also obtained documents and data.

II. Clarification of the facts

1. The Authority dated 14 October 2021, NAIH-7745-1/2021. in the order with file no

informed the Customer about the initiation of the data protection official procedure on the same day and to make a statement

called, and also CL of 2016 on general public administrative order. law (a

hereinafter: Ákr.) ordered by the Customer's website, the newsletter sender, based on § 108, paragraph (1)

and seizing the databases operating behind the SMS sender's systems.

The reason for the seizure was that in the case of deleting the personal data of the informant

takes place based on the calls made in the investigation procedure, there is a risk that it

The customer's databases will be deleted before the end of the official data protection procedure

whistleblower's personal data, which would endanger the success of clarifying the facts.

2. At the Customer's request, the Authority issued NAIH-7745-1/2021. specified in order with file number,

a 15-day deadline for responding, dated November 15, 2021, NAIH-7745-3/2021.

on the basis of his order with file number, he extended it by 20 days, until November 23, 2021, by

that the Authority is unable to extend the deadline beyond 20 days

to assure.

However, the Customer did not respond to NAIH-7745-1/2021 until December 15, 2021. case file number

to the questions asked in its order, despite the fact that the Authority extended the deadline

with NAIH-7745-3/2021. the return receipt returned to the Authority

according to his testimony, the Customer received it on November 23, 2021, and the extended deadline

several weeks have passed since then.

Therefore, the Authority dated 15 December 2021, NAIH-7745-4/2021. in the order with file no

obliged the Client to pay a procedural fine of HUF two hundred thousand, and again

called to make a statement NAIH-7745-1/2021. on the questions asked in order no.

The Customer provided information in a letter filed with the Authority on December 16, 2021.

Subsequently, the Authority dated February 11, 2022, NAIH-406-3/2022. case file number

ordered the Customer to make a statement again, as the clarification of the facts

it became necessary to answer additional questions. The Client at the Authority 2022.

provided information in his letter filed on March 17.

3. After reviewing what was written in the Customer's statement, it became necessary to clarify additional questions,

therefore, the Authority dated 22 June 2022, NAIH-406-6/2022. again in order no

invited the Customer to make a statement.

The Customer's statement was filed in the Authority's document management system on July 27, 2022.

4. Furthermore, in view of the fact that the official data protection procedure was preceded by the whistleblower

initiated, NAIH-2611/2021. investigation procedure was initiated, which is also the present procedure

in part, its subject, thus the present case, directly affects the rights and legitimate interests of the whistleblower, therefore the

Authority

the Akr. Based on Section 10 (1), dated June 24, 2022, NAIH-406-9/2022. case file number

granted the applicant legal status as a client in his order, dated June 22, 2022,

NAIH-406-6/2022. he also notified the Customer in his order with case file number.

5

fact

during clarification

uncovered evidence is

5. In addition, in this official data protection procedure, the employee of the Authority, Art. Section 62 (3)

subject to paragraph (1) of § 71, the Ákr. made a note based on § 78

on the fact finding that this data protection is used during decision-making

NAIH-2611/2021 prior to official proceedings. the entire file of the investigation procedure started under no. THE

a copy of the documents of the examination procedures is attached to the memorandum.

6. An employee of the Authority also prepared a note on May 10, 2022, stating that the

Based on the customer's statements, it is likely that a data protection incident occurred, given that

that the Customer had to restore their customer data from a backup after a ransomware attack

infected your IT system.

7. Furthermore, on June 17, 2022, an employee of the Authority made a note stating that

made a test registration or a test purchase on the [...] page, in order to information

be available, how the Customer provides information on the site about data subject rights,

especially about the possibility of erasing personal data.

8. The Authority subsequently, based on the evidence available to it, on September 2, 2022.

dated, NAIH-406-11/2022. informed the Client in his order with file number that

in the official data protection procedure, the evidentiary procedure has been completed and he drew your attention to the fact

that

the

of the rules of document inspection

taking it into account, you can get to know and make further evidentiary motions. The Authority

informed the Applicant about the same in NAIH-406-12/2022, dated September 5, 2022.

in the order with file no.

9. The Customer - after the Authority in its order dated September 30, 2022.

on the evening of October 11 or the inadequacy of this date would have provided it for October 13

inspection of documents, however, it failed, as the Client only on October 13, 2022

delivery took place - on November 8, 2022, the Authority exercised its right to inspect documents

at its registered office, which procedural act is referred to in NAIH-406-19/2022. a report with case file number was prepared.

After reviewing the documents, the Customer made in his letter filed on November 17, 2022

statement.

The whistleblower did not exercise his right to inspect the documents, as well as to request additional statements and evidence

neither did

10. Based on its declarations, the Customer has regulations that also cover the rights of stakeholders -

which he made available to the Authority - which dated May 25, 2018 "general

point X of the data protection regulations" provides for the governing procedure in the event of a request by the data subject,

practically quoting what is written in Article 12 of the General Data Protection Regulation.

According to the Customer's statement, on the basis of these rules, if someone informs the Customer by e-mail

that you do not wish to receive newsletters (no more than 2-3 letters per month), the newsletter sender

the Customer deletes it from the system as soon as possible, but within 30 days at the latest. According to his statement, in the case of the whistleblower, the Client realized it late, and the whistleblower did not correctly state that he no longer wants to unsubscribe from the newsletter, but calls it a newsletter through the customer card system also sent general informational system messages, including, for example, the offending name day greeting also a letter. As soon as this problem and misunderstanding was identified, it was deleted without delay the applicant's data were also removed from that data area.

According to the Customer's statement, the data management purpose of the general information system message is marketing

for data management

corresponds to, and within the marketing goal, contact or

it is sent for notification purposes. According to his statement, the legal basis for data processing is the data subject contribution.

According to the Customer's statement, following the notifier's notification on September 20, 2020, the Customer his colleague, on the instructions of the executive, deleted the personal data of the whistleblower, which are further

handling is not required by law, so your e-mail address and

phone number. This means that the deletion of the newsletter program called Webpigeon,

from the version 8 software data list and the Customer's internal software data list, i.e. the

marketing and the newsletter was done from a database.

According to the Customer's statement, at the following time, after a system update at the beginning of November hacker attack on your site. So that the ransomware does not know personal data

to obtain, and the Customer can continue to operate, a previous one, even personal to the whistleblower the status as of the time before the deletion of the data was restored, which is the notifier caused the problem in this case. The whistleblower's personal data are then back in the system were, so you received a message from the Customer on November 20, 2020. After that - his statement according to - in connection with the newsletter, the notifier used a signal again, therefore the Customer deleted his e-mail

address

newsletter database (from the data list of Webgalamb software and the Customer's internal software

from your data list).

According to the Customer's statement, the notifier will then receive a name day greeting on January 28, 2021

received a system message, then on March 9 and June 8, 2021, the

From a customer, not a newsletter. However, the whistleblower indicated in January that he had received a newsletter.

At that time, the Customer searched in vain, but did not find a newsletter sent out, as it was not a newsletter, but

a system message has been sent. However, this misunderstanding came to light in June, after which

the Customer deleted all personal information from all data groups - marketing and newsletter database

data to the notifier, the storage of which is not mandatory under the law (deletion in this case is

in both cases, it was made from the data list of the Web Pigeon software and from the Customer's internal software data list

it).

According to the Customer's statement, it is also possible to unsubscribe from electronic system messages,

which appears as an option at the end of every system message by attaching a link. With this

the whistleblower was never alive, as was the case with the newsletters.

According to the Customer's statement, the Customer currently manages the following personal data of the notifier:

-

data of your order (order number, total amount, number of products and price,

delivery method and cost, customer card number, account number, transaction code - Simple

OTP, payment made, date of creation and modification)

- data of the notifier as customer, billing and delivery data (name, country and

postal code, city and address, data provided as delivery data - name/requested time/address).

According to the Customer's statement, the name and address of the natural person's customers and buyers, a

In relation to the serial number of the issued invoice, the legal basis for the processing of personal data is a legal obligation

fulfillment (VAT Act § 159 (1)), the purpose of use of the personal data is the invoice

determining the mandatory data content, issuing invoices, related accounting tasks

supply.

According to the Customer's statement, the data of the placed order (order number, ordered products, price and total value of products), name, address, delivery address, registered office, business card number, original producer certificate number, order total, delivery method and cost, payment method, transaction code, in the case of data where payment has been made, the legal basis for data management is a contract fulfilment, the purpose of data management is to maintain contact, assert claims arising from the contract, ensuring compliance with contractual obligations.

According to the Customer's declaration, the way and characteristics of personal data are stored by the Customer included in its general data protection policy. Furthermore, the Customer is related to the website customer data, personal data stored in the newsletter and SMS sending systems, the own, web, it is managed in its uniquely developed software, from which the system also sends SMS messages. The client as a newsletter sending program, it uses version 8 of the above-mentioned Webpigeon program, while version of the customer card system v. 3.15.1.

According to the Customer's statement, with the Customer's website, as well as the newsletter sender and SMS sender system data on rented virtual and physical servers located in Hungary store it. The Customer works with a website development and maintenance company in connection with the rental of storage spaces together.

According to the Customer's declaration, with the website, its operation and the contents available on it editing, as well as synchronizing customer data and the newsletter software related tasks are performed by the Customer's internal employees. An external enterprise that subcontractor, authorized person who helps the Customer as a data processor, as it is on the website it is also mentioned in the information available, there is only one, [...] (headquarters: [...]; company registration number: [...]), which performs the maintenance of the website and the sending of newsletters and performs periodic IT tasks

away.

Furthermore, according to the Customer's statement, there was no other person other than the whistleblower who was personal

would have requested the deletion of his data, neither during the examined period nor afterwards.

In connection with the imposition of a possible data protection fine, according to the Customer's statement, in a row for the fifth year, it has recorded a loss of between HUF 40-90 million. This loss is borne by the Customer and the its owner is trying to finance it on its own and from external sources, but this has been increasing lately harder. In addition, the Client's liabilities significantly exceed its assets has an estate. Unfavorable market changes that have occurred in the past (directory rise, inflation above 10% within six months, elimination of KATA, beginning of economic recession, increase in loan interest rates) make it more difficult for the Customer to operate. The Customer shall verify these sent the accounts of the last three closed years.

In addition to all of this, the Customer asked for the following to be taken into account: "We have no interest and our intention to disturb our existing customers turned out this way completely by accident and this is the only one it can also be seen from the complaint addressed to us. Our goal is the long-term good relationship of our customers with us for the sake of long-term business relationships. Harassing and bombarding customers unwisely is marketing with campaigns is not our creed, please take this into account for a possible fine at the imposition!"

The Authority also reviewed the "general data protection regulations" - Annex No. 2 of which "with the Customer's economic activity related data management information" - and also dated May 25, 2018 "data protection information sheet". The latter information is available on the Customer's website2 dated April 8, 2019, which the Authority's employee viewed during the test registration. Furthermore, the Authority in 2019. also reviewed the general terms and conditions of the contract dated April 8th (hereinafter referred to as the General Terms and Conditions)3.

III. Applicable legal provisions

Based on Article 2 (1) of the General Data Protection Regulation, the general data protection regulation must be applied to the automated processing of personal data in whole or in part processing, as well as the processing of those personal data in a non-automated manner for handling, which are part of a registration system, or which are a they want to make it part of the registration system.

Infotv. Pursuant to § 2, paragraph (2), the general data protection regulation is indicated there shall be applied with the additions specified in the provisions.

Infotv. According to § 38, paragraph (2), the Authority is responsible for the protection of personal data, as well as for learning data of public interest and public in the public interest law

2 The data management information is available from the following link: [...]

3 The assf is available from the following link: [...]

control and promotion of its validity, as well as personal data within the European Union facilitating its free flow.

Infotv. Pursuant to Section 38 (2a) of the General Data Protection Regulation, the supervisory authority tasks and powers established for legal entities under the jurisdiction of Hungary as defined in the general data protection regulation and this law, a Exercised by authority.

Infotv. Pursuant to § 38, paragraph (3) point b), according to § 38, paragraphs (2) and (2a) within the scope of his duties, as defined in this law, especially at the request of the data subject and conducts a data protection official procedure ex officio.

Infotv. According to Section 60 (1), enforcement of the right to the protection of personal data in order to do so, the Authority initiates an official data protection procedure at the request of the data subject and may initiate official data protection proceedings ex officio.

The Akr. On the basis of § 103, paragraph (1), the application was initiated in the ex officio proceedings of this law

its provisions on procedures shall be applied with the exceptions contained in this chapter.

In the absence of a different provision of the General Data Protection Regulation, data protection initiated upon request for official procedure, the Acr. provisions shall be applied with the deviations specified in Infotv.

Pursuant to Article 4, point 1 of the General Data Protection Regulation: "personal data": you are identified any information relating to an identifiable natural person ("data subject"); it is possible to identify the a a natural person who, directly or indirectly, in particular an identifier, for example name, number, location data, online identifier or physical, physiological, one or more related to your genetic, intellectual, economic, cultural or social identity can be identified based on a factor."

According to Article 4, point 2 of the General Data Protection Regulation: "data management": on personal data or any operation performed on data files in an automated or non-automated manner or set of operations, such as collection, recording, organization, segmentation, storage, transformation or change, query, insight, use, communication, transmission, distribution or otherwise by way of making it available, coordination or connection, restriction, deletion, or destruction."

Based on Article 4, point 7 of the General Data Protection Regulation: "data controller": the natural person legal entity, public authority, agency or any other body that is the personal data determines the goals and means of its management independently or together with others; if the data management its purposes and means are determined by EU or Member State law, the data controller or the data controller EU or member state law can also determine special aspects regarding its designation."

According to Article 4, point 11 of the General Data Protection Regulation: "consent of the data subject": the data subject voluntary, specific and clearly informed declaration of will, by which the relevant statement or confirmation is indicated by means of an unmistakably expressive act, to give his consent to the processing of his personal data."

Based on Article 5 (1) points a) and b) of the General Data Protection Regulation: "Personal data:

a) must be handled legally and fairly, as well as in a transparent manner for the data subject

conduct ("legality, due process and transparency");

b) should be collected only for specific, clear and legal purposes, and should not be processed

in a manner inconsistent with these purposes; in accordance with Article 89 (1) no

is considered incompatible with the original purpose for the purpose of archiving in the public interest, scientific

and further data processing for historical research or statistical purposes ("for purpose

constraint").

9

Pursuant to Article 5 (2) of the General Data Protection Regulation: "The data controller is responsible for (1)

for compliance with paragraph and must also be able to demonstrate this compliance

("accountability")."

According to Article 6 (1) of the General Data Protection Regulation: "Management of personal data

it is only legal if and to the extent that at least one of the following is fulfilled:

a) the data subject has given his consent to the processing of his personal data for one or more specific purposes

for its treatment;

b) data management is necessary for the performance of a contract in which the data subject is one of the parties,

or to take steps at the request of the data subject prior to the conclusion of the contract

required;

c) data management is necessary to fulfill the legal obligation of the data controller;

d) the data processing is for the vital interests of the data subject or another natural person

necessary for its protection;

e) the data management is in the public interest or for the exercise of public authority delegated to the data controller

necessary for the execution of the task carried out in the context of;

f) data management to enforce the legitimate interests of the data controller or a third party

necessary, unless the interests of the data subject take precedence over these interests

or fundamental rights and freedoms that require the protection of personal data,

especially if a child is involved.

Point f) of the first subparagraph cannot be applied by public authorities in the performance of their duties

for data management."

Based on Article 7 of the General Data Protection Regulation: "(1) If data management is based on consent, it

data controller must be able to prove that the data subject's personal data

contributed to its treatment.

(2) If the data subject gives his consent in the context of a written statement that for other matters

also applies to consent

application for these other matters clearly

must be presented in a distinguishable manner, in an understandable and easily accessible form, clear and

with simple language. Any part of such statement containing the data subject's consent,

which violates this regulation, is not binding.

(3) The data subject is entitled to withdraw his consent at any time. The consent

its withdrawal does not affect the legality of data processing based on consent, prior to its withdrawal.

Before giving consent, the data subject must be informed of this. Withdrawal of consent

it should be possible in the same easy way as to enter it.

(4) In determining whether consent is voluntary, to the greatest extent possible

take into account the fact, among other things, that the performance of the contract - including

also the provision of services - whether it was set as a condition for the processing of such personal data

consent, which are not necessary for the performance of the contract."

Pursuant to paragraphs (1)-(6) of Article 12 of the General Data Protection Regulation: "(1) The data controller

takes appropriate measures to ensure that the personal data is provided to the data subject

all the information referred to in Articles 13 and 14 and Articles 15-22 and 34.

each piece of information according to Article is concise, transparent, comprehensible and easily accessible

provide it in a clear and comprehensible form, especially addressed to children

for any information. The information in writing or otherwise - including where applicable

the electronic way must also be entered. Verbal information can also be provided at the request of the data subject, provided

that

that the identity of the data subject was verified in another way.

(2) The data controller facilitates the relevant 15-22. the exercise of his rights according to art. Article 11 (2)

in the cases mentioned in paragraph 15-22 of the relevant to exercise his rights according to art

may not refuse to fulfill your request, unless you prove that the person concerned

cannot be identified.

(3) The data controller without undue delay, but in any case from the receipt of the request

informs the person concerned within one month of the 15-22 brought as a result of a request pursuant to art

measures. If necessary, taking into account the complexity of the application and the requests

number, this deadline can be extended by another two months. About the extension of the deadline

the data controller, indicating the reasons for the delay, from the date of receipt of the request

informs the person concerned within a month. If the person concerned submitted the application electronically, a

if possible, information must be provided electronically, unless the data subject requests otherwise

asks for

(4) If the data controller does not take measures following the data subject's request, without delay, but

informs the person concerned no later than one month from the date of receipt of the request

about the reasons for the failure to take action, as well as about the fact that the person concerned can submit a complaint to a

with a supervisory authority, and can exercise his right to judicial redress

(5) The information according to Articles 13 and 14 and Articles 15–22 and information according to Article 34 and

measure must be provided free of charge. If the data subject's request is clearly unfounded

- especially due to its repetitive nature - excessive, the data controller, taking into account the requested information or

for administrative costs associated with providing information or taking the requested measure:

a) may charge a fee of a reasonable amount, or

b) may refuse to take action based on the request.

It is the responsibility of the data controller to prove that the request is clearly unfounded or excessive.

(6) Without prejudice to Article 11, if the data controller has well-founded doubts regarding Articles 15-21. article
in relation to the identity of the natural person who submitted the application, further, the person concerned
you may request the provision of information necessary to confirm your identity."
According to Article 13 of the General Data Protection Regulation: "(1) If the data subject's personal
data is collected from the data subject, the data controller at the time of obtaining the personal data
provides all of the following information to the data subject:
a) the identity and contact details of the data controller and, if any, the representative of the data controller;
b) contact details of the data protection officer, if any;
c) the purpose of the planned processing of personal data and the legal basis of data processing;
d) in the case of data management based on point f) of paragraph (1) of Article 6, the data controller or a third party
legitimate interests of a party;
e) where applicable, recipients of personal data, or categories of recipients, if any;
f) where appropriate, the fact that the data controller is a third country or an international organization
wishes for
and compliance of the Commission
existence or absence of its decision, or in Article 46, Article 47 or Article 49 (1)
in the case of data transfer referred to in the second subparagraph of paragraph
indication of guarantees, as well as the methods for obtaining a copy of them or that
reference to their availability.
(2) In addition to the information mentioned in paragraph (1), the data controller is the personal data
at the time of acquisition, in order to ensure fair and transparent data management
ensure, informs the data subject of the following additional information:
a) on the period of storage of personal data, or if this is not possible, this period
aspects of its definition;
b) the data subject's right to request from the data controller the personal data relating to him
access to data, their correction, deletion or restriction of processing, and

you can object to the processing of such personal data, as well as to the data portability concerned

about his right;

c) based on point a) of Article 6 (1) or point a) of Article 9 (2)

in the case of data management, the right to withdraw consent at any time, which

it does not affect the legality of data processing carried out on the basis of consent before the withdrawal;

d) on the right to submit a complaint to the supervisory authority;

e) that the provision of personal data is a legal or contractual obligation

is a basis or a prerequisite for concluding a contract, and whether the person concerned is obliged to the personal

to provide data, and what possible consequences the provision of data may entail

failure to do so;

f) the fact of automated decision-making referred to in paragraphs (1) and (4) of Article 22, including

also profiling, and at least in these cases to the applied logic and that

comprehensible information regarding the significance of such data management and the data subject

looking at the expected consequences.

(3) If the data controller performs additional data processing on personal data for a purpose other than the purpose of their

collection

wish to perform, you must inform the data subject of this difference before further data processing

purpose and all relevant additional information mentioned in paragraph (2).

transmit personal data,

11

(4) Paragraphs (1), (2) and (3) do not apply if and to what extent the person concerned is already involved

has the information."

Based on Article 17 of the General Data Protection Regulation: "(1) The data subject has the right to, upon request

the data controller shall delete the personal data relating to him without undue delay, that is

and the data controller is obliged to provide the personal data concerning the data subject without justification

delete it without delay if any of the following reasons apply:

a) the personal data are no longer needed for the purpose for which they were collected or otherwise

treated in a manner;

b) the data subject withdraws it pursuant to point a) of Article 6 (1) or point a) of Article 9 (2)

point, the consent that forms the basis of the data management, and the data management has nothing else

its legal basis;

c) the data subject objects to the data processing based on Article 21(1) and there is no priority

enjoying a legitimate reason for data processing, or the data subject objects on the basis of Article 21 (2)

against data management;

d) personal data were handled unlawfully;

e) the personal data is legal as prescribed by EU or member state law applicable to the data controller

must be deleted to fulfill an obligation;

f) to collect personal data with the information society referred to in paragraph 1 of Article 8

took place in connection with the offering of related services.

(2) If the data controller has disclosed the personal data and pursuant to paragraph (1) it

must be deleted, taking into account the available technology and the costs of implementation

takes the reasonably expected steps - including technical measures - for it

in order to inform the data controllers handling the data that the data subject has requested from them

links to the personal data in question or copies of these personal data, or

deletion of its duplicate.

(3) Paragraphs (1) and (2) do not apply if data management is necessary:

a) for the purpose of exercising the right to freedom of expression and information;

b) EU or Member State law applicable to the data controller, which prescribes the processing of personal data

fulfillment of the obligation according to, or in the public interest or public authority entrusted to the data controller

for the purpose of performing a task performed in the context of exercising a driver's license;

c) in accordance with points h) and i) of Article 9 (2) and Article 9 (3)

on the basis of public interest in the field of public health;

d) in accordance with Article 89 (1) for the purpose of archiving in the public interest, scientific and

for historical research purposes or for statistical purposes, if the right referred to in paragraph (1).

would likely make this data management impossible or seriously jeopardize it; obsession

e) to present, enforce and defend legal claims."

Pursuant to Article 21 of the General Data Protection Regulation: "(1) The data subject is entitled to have his/her

object to your personal data at any time for reasons related to your situation in accordance with Article 6 (1)

against treatment based on points e) or f), including the aforementioned provisions

based profiling as well. In this case, the data controller may not process the personal data

further, unless the data controller proves that the data processing is legitimate with such coercive force

justified by reasons that take precedence over the interests, rights and freedoms of the data subject

against, or for the presentation, enforcement or defense of legal claims

are connected.

(2) If personal data is processed for direct business acquisition, the data subject is entitled

to object at any time to the processing of his personal data for this purpose,

including profiling, if it is related to direct business acquisition.

(3) If the data subject objects to the processing of personal data for direct business acquisition

against, then the personal data can no longer be processed for this purpose.

(4) The right referred to in paragraphs (1) and (2) shall be exercised no later than the first contact with the data subject

its attention must be specifically drawn to it, and the relevant information must be provided clearly

and must be displayed separately from all other information.

(5) In connection with the use of services related to the information society and

deviating from Directive 2002/58/EC, the data subject has the right to protest based on technical specifications

you can also practice with automated tools.

(6) If personal data are processed in accordance with Article 89 (1) scientific and

is carried out for historical research purposes or for statistical purposes, the data subject is entitled to have his/her own

for reasons related to your situation, you may object to the processing of your personal data,

unless the data processing is for the purpose of performing a task carried out for reasons of public interest

need."

According to Article 23 (1) of the General Data Protection Regulation: "You belong to the data controller

EU or Member State law applicable to the data processor may be limited by legislative measures

12-22 Article and Article 34, as well as Articles 12–22. with the rights specified in Article and

with regard to its provisions in accordance with obligations, the rights contained in Article 5 and

scope of obligations, if the restriction respects fundamental rights and freedoms

its essential content, as well as the necessary and proportionate measure to protect the following one

in a democratic society:

a) national security;

b) national defense;

c) public safety;

d) prevention, investigation, detection or prosecution of crimes, or

enforcement of criminal sanctions, including against threats to public safety

protection and prevention of these dangers;

e) other important general public interest objectives of the Union or a member state, in particular

An important economic or financial interest of the Union or a member state, including monetary, a

budgetary and taxation issues, public health and social security;

f) protection of judicial independence and judicial proceedings;

g) in the case of regulated occupations, the prevention, investigation and detection of ethical violations

and conducting related procedures;

h) in the cases mentioned in points a)–e) and g) – even occasionally – public authority tasks

control, inspection or regulatory activities related to its provision;

i) the protection of the data subject or the protection of the rights and freedoms of others;

j) enforcement of civil law claims."

Based on Article 58 (2) of the General Data Protection Regulation: "The supervisory authority is corrective

acting within its competence:

a) warns the data manager or the data processor that some planned data processing

its activities are likely to violate the provisions of this regulation;

b) condemns the data manager or the data processor if its data management activities

violated the provisions of this regulation;

c) instructs the data manager or the data processor to comply with this regulation for the data subject

your request to exercise your rights under;

d) instructs the data manager or the data processor that its data management operations - where applicable

in a specified manner and specified

within a period of time - harmonized by this regulation

with its provisions;

e) instructs the data controller to inform the data subject about the data protection incident;

f) temporarily or permanently restricts data management, including the prohibition of data management;

g) in accordance with the provisions of Articles 16, 17 and 18, orders personal data

rectification or deletion, or limitation of data management, as well as Article 17 (2)

in accordance with paragraph and Article 19, orders the notification of the recipients with whom

or with which the personal data was disclosed;

h) revokes the certificate or instructs the certification body to comply with Articles 42 and 43

to withdraw a duly issued certificate or instruct the certification body not to issue it

issue the certificate if the conditions for the certification are not or are no longer met;

i) imposes an administrative fine in accordance with Article 83, depending on the circumstances of the given case

in addition to or instead of the measures mentioned in this paragraph; and

j) orders the flow of data to a recipient in a third country or an international organization

suspension."

Pursuant to Article 77 (1) of the General Data Protection Regulation, other administrative or

without prejudice to judicial remedies, all interested parties are entitled to file a complaint

13

with a supervisory authority - in particular your usual place of residence, place of work or

in the Member State where the alleged infringement took place - if, according to the judgment of the data subject, the relevant

processing of personal data violates this regulation.

According to Article 83 (2) and (5) of the General Data Protection Regulation: "[…]

(2) Depending on the circumstances of the given case, the administrative fines of Article 58 (2)

It must be imposed in addition to or instead of the measures mentioned in points a)-h) and j). When deciding whether

whether it is necessary to impose an administrative fine, and the amount of the administrative fine

in each case, the following must be taken into account:

a) the nature, severity and duration of the infringement, taking into account the data management in question

nature, scope or purpose, as well as the number of persons affected by the infringement, as well as the

the extent of the damage they have suffered;

b) the intentional or negligent nature of the infringement;

c) mitigating the damage suffered by the data controller or the data processor

any action taken in order to;

d) the degree of responsibility of the data manager or data processor, taking into account the 25.

and technical and organizational measures taken pursuant to Article 32;

e) relevant violations previously committed by the data controller or data processor;

f) with the supervisory authority to remedy the violation and the possible negative effects of the violation

extent of cooperation to mitigate;

g) categories of personal data affected by the infringement;

h) the manner in which the supervisory authority became aware of the violation, in particular the fact that

whether the data controller or the data processor reported the violation, and if so, what kind

with detail;

i) if against the relevant data controller or data processor earlier - in the same subject

- one of the measures referred to in Article 58 (2) was ordered, in question

compliance with measures;

j) whether the data controller or the data processor considered itself approved according to Article 40

to codes of conduct or approved certification mechanisms under Article 42;

as well as

k) other aggravating or mitigating factors relevant to the circumstances of the case, for example a

financial benefit obtained or avoided as a direct or indirect consequence of infringement

loss.

[…]

(5) Violation of the following provisions - in accordance with paragraph (2) - at most 20,000

with an administrative fine of EUR 000 or, in the case of businesses, the previous financial year

shall be subject to an amount of no more than 4% of its total annual turnover on the world market, provided that a

of the two, the higher amount must be imposed:

a) the principles of data management - including the conditions of consent - in accordance with Articles 5, 6, 7 and 9;

b) the rights of the data subjects in Articles 12–22. in accordance with Article;

c) transfer of personal data to a recipient in a third country or an international organization

forwarding to 44–49. in accordance with Article;

d) IX. obligations according to the law of the Member States adopted on the basis of chapter;

e) the instruction of the supervisory authority according to Article 58 (2), and data management

temporary or permanent restriction or suspension of data flow

failure to comply with its notice or access in violation of Article 58 (1).

failure to provide.

[...]"

Infotv. On the basis of § 71, paragraph (2): "The Authority lawfully acquired during its procedures

document, data or other means of proof can be used in other proceedings."

VAT TV. Pursuant to § 159, paragraph (1): "The taxpayer is obliged - unless this law states otherwise

provides - for the product sale and service provision according to point a) of § 2, the product

for the purchaser or user of the service, if you are a person other than the taxable person

organization, to ensure the issuance of an invoice."

14

must be considered and which

According to paragraphs (1)-(2) of § 169 of the Szt.: "(1) The entrepreneur prepared a report for the business year, the

business report, as well as the supporting inventory, evaluation, ledger extract, and a

a logbook or other records that meet the requirements of the law can be read

form must be kept for at least 8 years.

(2) Accounting documents directly and indirectly supporting the accounting

(including ledger accounts, analytical and detailed records), for at least 8 years

must be readable, retrievable by reference to the accounting records

keep."

ARC. Decision

1. Based on the definitions of the General Data Protection Regulation, the natural person

data related to orders and contact are personal data, the personal

and any operation performed on data is considered data management.

2. Article 5 of the General Data Protection Regulation contains the main principles that a

during the processing of personal data

continuously

must apply during data management. Article 5 (2) of the General Data Protection Regulation

following the requirement of accountability according to the data controller is responsible for data protection

for compliance with the principles and must be able to demonstrate this compliance. Based on that, it is

the data controller is obliged to document and record the data processing in such a way that its legality

can be proved afterwards.

Purpose-bound data management according to Article 5 (1) point b) of the General Data Protection Regulation

following its principle, the processing of personal data is only specified, clear and legal
can be done on purpose. In this case, such a legitimate data management purpose is marketing, a
sending newsletters, sending system messages, as well as Szt. and Áfa tv. invoice and receipt
preservation obligation.
An additional requirement for the legality of data management is that the data management is general
can be done by referring to a legal basis according to Article 6 (1) of the Data Protection Regulation.
In the present case, the Customer operates an online store, which it manages for several purposes
personal data. After the notifier purchased a different on September 7, 2020
received messages from the Customer to his e-mail address or phone number in the form of SMS. THE
Based on the information available to the authority, these came from three different sources
to the notifier, given that the Customer operates three separate systems: a website
database, a newsletter sending database and an SMS sending system.
IV.1. Obligation to keep invoices and receipts
In connection with the obligation to keep invoices and receipts, the Customer shall comply with the Tax and VAT Act.
prescribed by legal
referred to the legal basis of obligation.
The legal basis for data management related to the obligation to retain invoices and receipts is the general one
may be a legal obligation according to Article 6 (1) point c) of the Data Protection Regulation, which is legal
obligation is prescribed by Paragraphs (1)-(2) of § 169 of the Civil Code. Based on this, the entrepreneur, i.e. the Customer
the report prepared for the business year, the business report, as well as the inventory supporting them,
assessment, ledger extract, and the log book, or other requirements of the law
must keep appropriate records in legible form for at least 8 years. The accounting
accounting documents directly and indirectly supporting settlement (including ledger
invoices, analytical and detailed records as well), must be read for at least 8 years
form, to preserve it in a retrievable way based on the reference of the accounting records.

VAT TV. - among other things - point e) of § 169 contains the mandatory content elements of the invoice, which

according to the invoice must contain the name and address of the user of the service.

The Szt. and VAT tv. based on its provisions, therefore, the Client is entitled to the notifier – and generally any

customer - name and address data - and the invoices containing them - must be kept for at least 8

years, but not your other personal data - e-mail address, phone number.

On this, Szt. and VAT tv. by storing personal data that must be kept according to

in its general practice, as well as within the personal data of the applicant's request for deletion

the Customer did not commit a legal violation by not complying.

IV.2. Marketing letters

1. The Customer is responsible for the sending of newsletters and system messages that he classifies as marketing purposes.

referred to the legal basis of consent as the legal basis for data management.

The Authority's legal basis for data management for marketing purposes is Article 6 (1) of the General Data Protection

Regulation

the legal basis for stakeholder consent according to paragraph a) or point f) of Article 6 paragraph (1).

considers the legal basis of legitimate interest as appropriate.

In the case of reference to the legal basis of the consent, the consent is the general data protection

according to its definition according to the decree, the following basic requirements can be established:

- Consent must be based on adequate information. The appropriate information is

through which the affected parties learn about their personal data

data management, and the right to self-determination of information through information

take effect: data processing can be lawful, the circumstances of which are in front of the data subjects

are fully known. The requirement to inform the data subject in advance is general

13-14 of the data protection decree. article details.

- One of the most important components of the validity of the consent is the will of the person concerned

its voluntariness, its freedom from external influence, which is realized when it is real

electoral

option is available to the person concerned. If the consent

consequences undermine the individual's freedom of choice, consent is not considered

as a volunteer.

- A concrete, clear, unmistakable statement or confirmation of the will of the person concerned

the requirement to declare it through an expressive act means on the one hand that

consent must be active conduct, not an active conduct

[for example, not turning off a signal in a check box] no

can be considered a definite and unmistakable consent. On the other hand, it is clear and explicit

consent is also consent assigned to a purpose: specific, specific data management

can be considered as a contribution to the goal. As a general rule, the data is handled differently

cannot be used for this purpose.

In the case of data management based on consent - subject to Article 7 of the General Data Protection Regulation.

(3) of Article - it must be ensured that the data subject can withdraw his consent at any time

draw, and in view of this, he is also entitled to do so - subject to Article 17 of the General Data Protection Regulation

(1) point b) - that the data controller deletes the data without undue delay

relevant personal data.

In the case of reference to the legal basis of legitimate interest, personal data may be processed if the data management

necessary to enforce the legitimate interest of the data controller, unless with these interests

interests or fundamental rights and freedoms of the data subject shall take priority

which require the protection of personal data. The legitimate interest must actually exist

and must actually exist.

It is important that the data controller must carry out an interest assessment to refer to this legal basis4. The

carrying out an interest assessment involves a multi-step process, during which it is necessary to identify

the legitimate interest of the data controller, as well as the interest of the data subject, which is the counterpoint of the

weighting, is affected

fundamental right, and finally, based on the weighting, it must be established whether it can be treated as personal data. If, as a result of the consideration of interests, it can be determined that the data controller its legitimate interest precedes the data subject's right to the protection of personal data, it can be treated as such personal data.

In the case of data management based on legitimate interest, Article 17 (1) of the General Data Protection Regulation based on paragraph c) the data controller is obliged to delete the data subject's personal data, if the data subject is the data subject

- based on Article 21 (1) of the General Data Protection Regulation - objects to data processing,

and there is no overriding legitimate reason for data processing, or the data subject - Article 21 (2)

based on paragraph - objects to data processing for the purpose of direct business acquisition.

In this case, according to the above, the Customer is the newsletter sending and system message sending purposes The legal basis of data processing for the purpose of inclusive marketing is the data subject, that is, the notifier referred to his consent.

2. Pursuant to the above, one of the conditions for consent is that it is based on adequate information.

The Customer provided the Authority with the "general

data protection regulations" - Annex No. 2 of which "with the Customer's economic activity

related data management information" - and also dated May 25, 2018 "data protection

information sheet". The latter information is available on the Customer's website dated April 8, 2019.

After reviewing these documents, the Authority concludes that the "general data protection

regulations - and its Annex No. 2 - as well as those sent by the Customer and on its website

of the available "data protection information", only the "general data protection policy" is listed

data management purposes include the newsletter service and data management for marketing purposes, however, these purposes

apart from its definition, neither this regulation nor the additional document contains any

information about the Customer's data processing for marketing purposes. Article 13 of the General Data Protection Regulation (1)-(2), however, stipulates that if the personal data concerning the data subject is

are collected from the data subject, the data controller is the data subject at the time of obtaining the personal data

provides it for the purpose of data management and all its circumstances

information. However, one of the Customer's data protection content does not meet this requirement

document, including the information available on the website, as they do not contain any

information about data processing for marketing purposes.

The Authority therefore concludes that the Client, by not providing any information, is

in its data management information for the data subjects for marketing purposes, violated it

Article 13 (1)-(2) of the General Data Protection Regulation.

3. In view of the fact that the Customer did not provide information about data processing for marketing purposes,

the existence of which prior information is one of the conditions for the data subject's consent

legal basis can be legally invoked, the Authority determines that the Customer is without a legal basis

manages the personal data of those concerned with regard to data processing for marketing purposes, in violation

thereby Article 6 (1) point a) of the General Data Protection Regulation.

In order for the data management to be legal, the Customer must inform the data subjects a

about data processing for marketing purposes and you must ask for their consent or their consent

confirmation. In the absence of this, the Customer must take care of the personal data of the persons concerned

on the documented deletion of your data.

4 The Data Protection Working Group 6/2014 provides assistance in carrying out the interest assessment. No., according to

Article 7 of the Data Controller Directive 95/46/EC

its legitimate interests

available from the link: https://ec.europa.eu/justice/article-

29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf

his opinion on the concept of The opinion is below

4. The Authority also reviewed the ASF dated April 8, 2019 available on the Customer's website

too. Point 13 of this provides for data protection, according to which: "with data protection

related provisions in the “Data Management Information ([…])” on the websites of [...]

can be reached. By accepting the General Terms and Conditions, you declare that you have read the data protection information,

accepted, and for the data management purposes for which the Data Subject's consent is the legal basis, you a consent to data management. The data management purposes for the use of the website, newsletter by sending, ordering from the website, using a service, personal shopping are related."

The Authority's position in this regard is that because of the above, since the information sheet does not contains data management for marketing purposes, such as sending newsletters any information - thus this data management purpose itself and the general data protection regulation nor the additional information specified in Article 13, Paragraphs (1)-(2) - with the acceptance of the Ásf legally - in the absence of adequate information - you cannot consent to the sending of newsletters nor for related data management. In addition, the acceptance of the assf must be separated from the consent from its submission. Giving consent is a category of data protection law, it cannot become part of the assf as the acceptance of the assf also automatically means consent to data management.

Pursuant to Article 7 (2) of the General Data Protection Regulation, if the consent of the data subject give consent in the context of a written statement that also applies to other matters an application for this must be submitted in a way that is clearly distinguishable from these other cases, in an understandable and easily accessible form. Therefore, the contribution is required separately from the assf to acquire, separately for each data management purpose. Given that it is employed by the Client assf does not meet the above requirements, the Authority determines that the Customer is the general one violates Article 7 (2) of the Data Protection Regulation and requests the consent of the data subjects.

5. The Authority also investigated the Customer's 2020 on a separate case number (NAIH-5404/2022.) hacker attack and data protection incident in November, on the basis of which he established that a based on the available data, the incident probably did not pose a risk to those involved rights and freedoms, and the security of the data involved in the incident to the Customer

managed to restore from backup.

IV.3. Deletion of personal data of the notifier

The whistleblower requested the deletion of his personal data.

Data controller obligations related to the deletion of personal data are covered by general data protection

12 of the decree.

Based on Article 12 (3) of the General Data Protection Regulation, the data controller is unjustified

without delay, but in any case within one month of receipt of the request

is obliged to provide information on the measures taken on the basis of the request for deletion. Need

in this case, this deadline can be extended by another two months, upon the fact of the extension

and the reasons for the delay must be provided within one month of receiving the request

to provide to the data controller.

Pursuant to Article 12 (4) of the General Data Protection Regulation, if the data controller is the request

does not take action, then without delay, but no later than upon receipt of the request

must inform the data subject of the reasons for not taking the measure within one month,

and that the person concerned can file a complaint with the Authority or seek legal remedies

with his right.

According to Article 12 (5) of the General Data Protection Regulation, it is related to data subject rights

requests, such as the action taken following the request for deletion and the information about it

it must basically be provided free of charge. If the data subject's request is clearly unfounded

- especially due to its repetitive nature - excessive, the data controller, taking into account the requested information or

administrative costs associated with providing information or taking the requested measure,

may charge a reasonable fee or refuse to act on the request.

However, proving the clearly unfounded or excessive nature of the request is

is charged to the data controller.

Article 23 (1) of the General Data Protection Regulation also defines the special

cases, the existence of which may limit the rights of the data subject, such as the right to deletion.

In this case, according to the correspondence between the notifier and the Client available to the Authority

the whistleblower first requested his personal data by e-mail on September 20, 2020, at 6:24 p.m.

deletion from the Customer's own and connected systems. He received the same answer that same day, at 20:38

From the customer's representative that their request has been complied with.

The Client's statement to the Authority in this regard was that the whistleblower in September

after indicating it, an employee of the Client deleted it on the instructions of the executive

personal data, the further processing of which is not required by law

provision, so the Customer's marketing and newsletter e-mail address and telephone number have been deleted

from its database.

After that, in an electronic letter dated November 22, 2020, the whistleblower complained that

that on November 20, 2020, he received an SMS about a promotion from the Customer. In this letter, the whistleblower

asked the Customer's representative how he could have received the SMS in question

t if all your personal data has been deleted.

The Customer's managing director - following the notifier's letter of inquiry dated November 27, 2020 - 2020.

responded on November 30, according to which it was deleted in accordance with the complainant's request

your data from newsletter and other similar lists. However, the purchase data cannot be deleted

must be stored for a year. "Telephone numbers were integrated and text messages were sent to buyers who

in a certain period they bought […].” According to the Customer's letter, it is carelessness and that

due to the lack of combing, it may have happened that the informant received an SMS, however, based on his indication

they made sure to delete your phone number.

According to the Customer's statement submitted to the Authority, it was received during this period, at the beginning of

November

hacker attack on the Customer's side after a system update and due to its management

an earlier date, even before the deletion of the notifier's personal data, was restored

state, as a consequence of which the reporting person was once again in the system

data, such as your phone number and e-mail address. That is why you received a message from the Customer at the end of November,

following its indication, the Customer deleted his e-mail address from the newsletter list. The client

according to his statement, this second request of the whistleblower concerned the database of the newsletter, so from this your personal data has been deleted - it is not mandatory to store it.

After all this, on January 28, 2021, the notifier received a name day greeting electronic letter

from the Customer, and then despite the fact that, according to his statement, he had previously unsubscribed

from customer card, customer card usage notification on March 9, 2021, and then on June 8, 2021

received an e-mail from the Customer with a subject line.

The Client's statement to the Authority in this regard was that these messages

they were system messages, not newsletters, at the same time - also according to his statement -

both types of letters are letters with marketing content. In January, the whistleblower indicated that it was a newsletter got At that time, the Customer searched in vain, but did not find a newsletter sent out, as it was not a newsletter, but a system message has been sent. However, this misunderstanding came to light in June, after which

the Customer has deleted all personal data of the notifier from all data groups, which

its storage is not required by law. The Customer did not state the exact date of this, a

According to information available to the Authority, at the same time, in the investigation procedure at the Authority

According to the screenshot attached to the letter filed on May 26, 2021, the Customer

the whistleblower's phone number and e-mail address were still available in his system at that time, while the

according to the screenshot attached to the letter filed in the official procedure on December 16, 2021

no.

19

The Authority's position in relation to all this is that the notifier is already the first, September 2020

In his letter of the 20th, the Customer requested the deletion of all his personal data, both his own and attached

systems, not just the newsletter sender's system. The whistleblower confirmed the same

His electronic letter of November 22, 2020, in which he inquired about how he could have received it

A text message from a customer even though he has deleted all his personal data.

Based on this, the Customer will receive all personal data of the notifier - phone number, e-mail

address - you should have deleted it from all your systems and lists, which you do not require to be stored

statutory provision.

A contradiction can also be established by the Customer's statement submitted in the investigation procedure,

respectively between the statement presented in the official procedure in the sense that the investigation

according to the statement submitted in the procedure, it was deleted from both the newsletter sender and the customer card

database

e-mail address of the applicant, and his telephone number from the delivery data, while in the official procedure

according to the statement submitted, only from the newsletter sending database, given that their interpretation

according to this, the deletion request was covered. Furthermore, on November 30, 2020, the Managing Director of the Client

informed the whistleblower that his personal data was deleted in accordance with his request from the newsletter and other

from similar lists.

A contradiction can also be established in relation to the fact that, according to the Customer's statement, a

the reporting party did not unsubscribe from newsletters or system messages on any occasion

case, at the same time, according to the whistleblower's statement, he attempted to

unsubscribe is

from a customer card, and nevertheless received on March 9, 2021 and then on June 8, 2021

card usage notification letter with subject designation.

In addition to all these contradictions, however, regarding the ascertainability of the infringement, the

the most important circumstance is that the notifier already for the very first time, on September 20, 2020

requested the deletion of all his personal data from all databases of the Customer, according to his request: "on this

by letter, I request the deletion of my personal data from both your and the attached systems!".

Even if as a result of the hacker attack referred to by the Customer in November 2020

the Customer's database was also restored, after which the whistleblower should have been taken into account

to the deletion requests previously and then repeatedly sent by

e-mail address and telephone number, and thus the Customer could not have sent it January 28, 2021,
on March 9 and then on June 8 additional letters and system messages with marketing content. THE
The Authority also emphasizes that the Client did not mention this in the investigation procedure
about a hacker attack and also to the whistleblower with carelessness and a lack of coordination,
that he received a text message despite his cancellation request, while he presented it to the Authority in the investigation
procedure
according to his statement, due to the regular updating of the newsletter and its connection to the website
the database was resynchronized, which is why the notifier could receive another inquiry. So the Customer
by not informing the whistleblower about the consequences of the hacker attack
in order to alleviate it, the database was restored to a previous state with his personal data,
instead, he cited inattention and lack of combing, for which he was repeatedly received
messages, did not provide adequate, real information to the whistleblower based on the stakeholder's request
measures taken, thus violating Article 12 (4) of the General Data Protection Regulation.
The Authority therefore instructs the Client to provide the reporter with appropriate information
about all measures taken based on your cancellation request.
Based on all of this, therefore, according to the Authority's point of view, the Client should notify September 2020
In view of your letter dated the 20th, you should have deleted all your personal data - including
your e-mail address and telephone number - from all your databases, except those related to the invoice,
personal data that must be stored. This is independent of whether there is an option for newsletters,
to unsubscribe from system messages, i.e. emails with marketing content, since the unsubscribe
to be distinguished from the exercise of the rights of the data subject because opting out does not mean at the same time a
deletion of personal data. On the other hand, even if the opt-out includes the personal

deletion of data, even then this cannot be ensured solely through unsubscribing, but must be sufficient
to the data subject's request even if he submits a separate request to the data controller.
The hacker attack referred to in November 2020, which concerns data protection

led to an incident,

may have contributed to the whistleblower receiving inquiries again in November 2020

However, he received inquiries from the client even after he indicated this also this month,

therefore, the Customer did not comply with the declarant's cancellation request either.

It can therefore be concluded that the Client did not comply with the request for cancellation twice by the notifier. THE

on September 20, 2020, the complainant first requested the deletion of all his personal data

From all customer databases and lists, and a second time on November 22, 2020. The client

however, on November 20, 2020, January 28, 2021, March 9, 2021, and then on June 8, 2021

also sent messages to the whistleblower by e-mail and SMS, despite the fact that 2020.

The Customer was also informed about this on September 20 and November 30, 2021

from his manager that he has deleted all his personal data.

Based on all of this, the Authority concludes that the Customer did not delete the

in view of the request of two notifiers, all of their personal data – e-mail address, telephone number –,

for the storage of which the Szt. and VAT is not obliged to do so, he violated it twice

Article 17 (1) point b) of the General Data Protection Regulation.

Considering that in the official procedure, attached to the letter of December 16, 2021

according to screenshots, the Customer no longer stores the e-mail address and telephone number of the notifier,

there is no need to order deletion.

IV.4. The general practice of fulfilling requests for the deletion of personal data and the

relevant information

1. The "general" dated May 25, 2018 provided to the Authority by

data protection regulations" IX. point 3.2. sub-section provides for the right to deletion, and section X

on the governing procedure in the event of a request by the data subject. Also dated May 25, 2018 - and it is

April 8, 2019 available on the customer's website - "data protection information" also lists

cases in which it is necessary to delete the data subject's personal data.

According to the Customer's statement, on the basis of these rules, if someone informs the Customer by e-mail

that you do not wish to receive newsletters (no more than 2-3 letters per month), the newsletter sender
the Customer deletes it from the system as soon as possible, but within 30 days at the latest.
However, according to the Customer's statement, there was no other person besides the whistleblower who was personal
would have requested the deletion of his data, neither during the examined period nor afterwards.
The Authority, accepting the Client's statement that no one other than the whistleblower lived personally
with his right to delete his data and after reviewing the regulations and information, the opposite
in the absence of evidence, no violation of the law is established, the general fulfillment of cancellation requests
regarding its practice, however, draws the attention of the Customer to IV.2 of this decision. in point
written in relation to the deletion of all personal data of a data subject
requests, then it is not enough to simply delete them from a database or unsubscribe
its absence cannot be an obstacle to the deletion of personal data. If the Customer is not clear
for the data subject's request, it is necessary to request additional information to ensure the data subject's right
in order to
At the same time, the Authority states that the regulations and information sheets affect data subject rights
its relevant parts are basically repeated verbatim in the general data protection regulation,
as well as those contained in Articles 12 and 17 thereof, without prejudice to the Customer's data management, and the
they would be specified for the fulfillment of stakeholder rights. The data protection policy is one
internal, containing the data management of the data controller and their circumstances, internal procedures

document, its addressees are basically the data manager and the legal relationship with him
standing persons. The data management information is intended for persons other than the data controller,
plain document, essentially a simplified data management policy, for those concerned
and information according to Article 13 (1)-(2) of the General Data Protection Regulation
can also be matched to its extract containing
The essence of the data management information is that the information provided by the data controller can be understood in it
the manner in which it complies with the legal requirements. Its special importance

there is public comprehensibility regarding the data subject's rights, since the data subject can live by knowing them with his right to informational self-determination, in the case of this case, for the deletion of his personal data with his right. The mere adoption of the legal provisions of the text of the data management information is stakeholder rights and the procedure for their exercise in general and this information also make it incomprehensible, complicated and difficult. 12 of the General Data Protection Regulation.

(1) specifically stipulates that the data controller shall take appropriate measures in order to comply with the provisions of Articles 13 and 14 concerning the processing of personal data for the data subject all the information mentioned in article 15-22. and each information according to Article 34 in a concise, transparent, comprehensible and easily accessible form, in a clear and understandable way provide it formulated. Given that the Customer did not comply with this requirement, violated Article 12 (1) of the General Data Protection Regulation.

2. The Authority also refers back to IV.2 of this decision. to those written in point, according to which the Customer does not provide information about its data processing for marketing purposes, which violates general data protection Article 13 (1)-(2) of the Decree.

IV.5. Cancellation of reservation

The Authority dated 14 October 2021, NAIH-7745-1/2021. in its order with case file no. Ordered by the Customer's website, the newsletter sender and the SMS sender based on § 108, paragraph (1) seizure of databases operating behind its systems.

The reason for the seizure was that in the case of deleting the personal data of the informant takes place based on the calls made in the investigation procedure, there is a risk that it The customer's databases will be deleted before the end of the official data protection procedure whistleblower's personal data, which would endanger the success of clarifying the facts.

According to the Customer's statement filed on December 16, 2021, it was canceled in June 2021 by the notifier your personal data. The Client did not state the exact date of this at the disposal of the Authority according to available information, at the same time in the investigation procedure to the Authority on May 26, 2021 according to the screen save attached to the registered letter, it will still be in the Customer's system at that time

the telephone number and e-mail address of the notifier were available, while in the official procedure December 2021
According to the screenshot attached to the letter filed on the 16th, no longer.
All of these, and based on the Customer's statement, the notifying invoice and receipt storage
non-obligatory personal data in June 2021, the official data protection procedure
were canceled before the date of its initiation and the order of seizure - October 14, 2021,
the seizure could not be carried out in relation to the declarant.
The reason for the seizure was thereby eliminated, and since the Authority made a decision on the merits of the case, a
Authority of the Ákr. Based on § 109, paragraph (1), point c) of the Customer's website, the newsletter sender and the
terminates the reservation of databases operating behind its SMS sending systems.
22
Sun. Legal actions
Based on Article 58 (2) point b) of the General Data Protection Regulation, the Authority establishes,
that the Customer is because the data management information on the website does not contain information
on data processing for marketing purposes, violated Article 13 (1)-(2) of the General Data Protection Regulation
paragraph.
Based on Article 58 (2) point d) of the General Data Protection Regulation, the Authority orders the
Client to provide appropriate, comprehensible and transparent information to those concerned
about all data management and their circumstances.
Based on Article 58 (2) point b) of the General Data Protection Regulation, the Authority establishes,
that the Customer handles the personal data of the data subjects for marketing purposes without a legal basis
regarding data management, in violation of Article 6 (1) of the General Data Protection Regulation
point a) of paragraph
Based on Article 58 (2) point b) of the General Data Protection Regulation, the Authority establishes,
that the Customer, because of the general terms and conditions of the contract (hereinafter referred to as
at the same time as its acceptance, the consent of the affected parties is considered to be given on all of them
for data management, which

legal basis is the consent of the person concerned, violated the general

Article 7 (2) of the Data Protection Regulation.

Based on Article 58 (2) point d) of the General Data Protection Regulation, the Authority orders the

Client to request data processing for marketing purposes in an appropriate manner

consent, as well as in the case of already started and ongoing data processing

confirmation of their consent, separate from the acceptance of the asf. In the absence of this

ensure the documented deletion of the personal data of the data subjects.

Based on Article 58 (2) point b) of the General Data Protection Regulation, the Authority establishes,

that the Customer is concerned because he did not provide adequate, true information to the whistleblower

on the measures taken based on your request, violated Article 12 (4) of the General Data Protection Regulation

paragraph.

Based on Article 58 (2) point b) of the General Data Protection Regulation, the Authority establishes,

that the Customer did not delete his e-mail address and telephone number at the request of the notifier

from all of its databases, violated Article 17 (1) paragraph b) of the General Data Protection Regulation

point.

Based on Article 58 (2) point c) of the General Data Protection Regulation, the Authority orders the

Customer to inform the notifier based on his request for deletion of personal data

about the measures taken.

Based on Article 58 (2) point b) of the General Data Protection Regulation, the Authority establishes,

that the Customer has violated it because he did not provide publicly comprehensible information about his data management

Article 12 (1) of the General Data Protection Regulation.

The Authority examined whether the imposition of a data protection fine against the Customer is justified. E

in the scope of the Authority, Article 83 (2) of the General Data Protection Regulation and Infotv. 75/A. §-

considered all the circumstances of the case on the basis of and established that it was revealed during the present procedure

in the case of legal violations, the warning is neither a proportionate nor a dissuasive sanction, therefore

a fine must be imposed.

When determining the amount of the fine, the Authority first of all took into account that

Violation committed by the customer Article 83 (5) point b) of the General Data Protection Regulation

is classified as a violation of the higher penalty category.

23

The Authority took it as an aggravating circumstance when determining the amount of the data protection fine

considering that

- in the absence of adequate information, the Customer handles it on the basis of invalid consents

the personal data of the data subjects with regard to data processing for marketing purposes [general

Article 83 (2) point a) of the Data Protection Regulation].

- despite the notifier's repeated request twice, his personal data was not deleted,

limiting the whistleblower's exercise of data subject rights [General Data Protection Regulation Article 83 (2)

paragraph point a)];

- non-fulfillment of the right of the affected party was caused by the Customer's careless behavior [general

Article 83 (2) point b) of the Data Protection Regulation];

- the Customer does not refer to his specific data management and related information in his data management information

provides information on information regarding the exercise of the rights of the data subject, but only

generally, formally, repeating the text of the general data protection regulation

[General Data Protection Regulation Article 83 (2) point d];

- in the investigation procedure of the Authority, the Client did not do what was required by the Authority

measures to ensure legal data management [general data protection

Regulation Article 83 (2) point f)].

The Authority took it as a mitigating circumstance when determining the amount of the data protection fine

considering that

- it cannot be determined in connection with the fulfillment of data subject rights - deletion of personal data

General illegal practice used by the customer [general data protection regulation 83.

Article (2)(k)];

- the rights of stakeholders did not arise in relation to stakeholders other than the reporting party

violation of rights related to the exercise of [General Data Protection Regulation Article 83 (2)

paragraph [General Data Protection Regulation Article 83 (2) point a)];

- not yet to convict the Customer for violating the general data protection regulation

took place [General Data Protection Regulation Article 83 (2) point e)];

- the personal data affected by the infringement, the telephone number and e-mail address, do not belong to

to the special category of personal data [General Data Protection Regulation Article 83 (2)

paragraph g)];

- the Authority exceeded the administrative deadline [General Data Protection Regulation Article 83 (2)

paragraph (k)].

The Authority did not consider it when determining the data protection fine imposed on the Client

as relevant according to Article 83 (2) c), h), i) and j) of the General Data Protection Regulation

circumstances, as they cannot be interpreted in relation to the specific case.

The net sales revenue of the Customer in 2021 was HUF 143 million, so the

the imposed data protection fine is far from the maximum fine that can be imposed.

VI. Other questions:

The Authority is Infotv. 60/A. taking into account paragraph (1) of § to clarify the facts

not the periods from the invitation to provide necessary data to its fulfillment

included in the administrative deadline. Based on this corrected deadline calculation, the 150 days

administrative deadline expired on May 6, 2022, compared to which the administrative deadline

twice as long will expire on January 13, 2023. The Authority oversteps the 150-day administrative deadline

assessed as a mitigating circumstance.

The competence of the Authority is set by Infotv. Paragraphs (2) and (2a) of § 38 define it, and its competence is

covers the entire territory of the country.

This decision of the Authority is based on Art. 80-81. § and Infotv. It is based on paragraph (1) of § 61. The decision

the Akr. Based on § 82, paragraph (1), it becomes final upon its publication. The Akr. § 112 and § 116 (1)

and paragraph (4) point d) and against the decision based on § 114. paragraph (1)

there is room for legal redress through an administrative lawsuit.

* * *

The Akr. According to § 135 of the

is obliged to pay if he does not fulfill his obligation to pay money within the deadline.

Act V of 2013 on the Civil Code 6:48 § (1) money owed

in the case of the obligee starting from the date of default in the calendar affected by the delay

is liable for late payment interest equal to the central bank base rate valid on the first day of the semester

to pay.

The rules of the administrative trial are set out in Act I of 2017 on the Administrative Procedure

hereinafter: Kp.) is defined. The Kp. Based on § 12, paragraph (1), by decision of the Authority

the administrative lawsuit against falls within the jurisdiction of the court, the lawsuit is referred to in the Kp. § 13, subsection

(3) a)

on the basis of subparagraph aa) of The Kp. Section 27 (1)

According to paragraph b) in a legal dispute in which the court has exclusive jurisdiction, the legal

representation is mandatory. The Kp. According to paragraph (6) of § 39, the submission of the statement of claim a

does not have the effect of postponing the entry into force of an administrative act.

The Kp. Paragraph (1) of Section 29 and, in view of this, CXXX of 2016 on the Code of Civil Procedure.

applicable according to § 604 of the Act, electronic administration and trust services

CCXXII of 2015 on its general rules. according to Section 9 (1) point b) of the Act, the customer

legal representative is obliged to maintain electronic contact.

The time and place of submitting the statement of claim is set by Kp. It is defined by § 39, paragraph (1). The trial

information about the possibility of an application for holding the Kp. It is based on paragraphs (1)-(2) of § 77.

The amount of the fee for the administrative lawsuit is determined by Act XCIII of 1990 on fees. law

(hereinafter: Itv.) 45/A. Section (1) defines. It is from the advance payment of the fee

Itv. Paragraph (1) of § 59 and point h) of § 62 (1) exempt the party initiating the procedure.

If the Customer fulfills the prescribed obligations and payment obligations in an appropriate manner
does not certify, the Authority considers that the obligation has not been fulfilled within the deadline. The Akr.
According to § 132, if the Customer has not fulfilled the obligations contained in the Authority's final decision
enough, it is enforceable. The Authority's decision in Art. according to § 82, paragraph (1) with the communication
becomes permanent. The Akr. Pursuant to § 133, enforcement - if it is a law or government decree
does not provide otherwise - it is ordered by the decision-making authority. The Akr. Pursuant to § 134 of
enforcement - if it is local in the case of a law, government decree or municipal authority
the regulation of the municipality does not provide otherwise - it is carried out by the state tax authority. Infotv.
Pursuant to § 61, paragraph (7), a specific action included in the Authority's decision
an obligation to perform, to engage in certain conduct, to tolerate or to cease
regarding the implementation of the decision, the Authority undertakes

Dated: Budapest, December 20, 2022.

Dr. Attila Péterfalvi

c. professor

president