Case number: NAIH-2732-2/2023.

Former case number: NAIH-2847/2022.

Subject: decision establishing a violation of law,

imposing a data protection fine

H A T A R O Z A T

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

(KASZ: [...].) represented by I&S Limited Kft. (headquarters: 1036 Budapest, Bécsi út 38-44. I. em.

Spandora Beauty Center, company registration number: 01-09-303223), (hereinafter: Company) the personal

on the protection of data in terms of processing and the free flow of such data, as well as a

in Regulation (EU) 2016/679 on the repeal of Directive 95/46/EC (hereinafter:

ex officio in connection with compliance with the provisions contained in the General Data Protection Regulation).

in the initiated data protection official procedure, the Authority makes the following decisions:

1.

2.

3.

4.

5.

The Authority states that the Company continuously records the work and the guests

breached points a) and b) of Article 5 (1) of the GDPR with its observation, and Article 6 (1)

paragraph, therefore the Authority prohibits camera data management in operators, as well as a

in diagnostic and examination rooms, and further instructs the Company that this decision

within 8 days of its becoming final, delete it in a documented way in the managers, as well as a

video recordings made in diagnostic and examination rooms.

The Authority finds that the Company has violated Article 13 (1)-(2) of the GDPR, as

it provided incorrect or misleading information in its information sheet and consultation data sheet

concerned about the management of their personal data, therefore the Authority instructs the Company to provide

appropriate, comprehensible and transparent information for those concerned about all data management and their circumstances.

The Authority determines that the Company operates the camera system and manages the data minimal default settings, personal data at the highest possible level by failing to provide the means necessary for its protection, violated the general Article 5, paragraph 1, Articles 24 and 25 of the data protection decree, as well as the system security by failing to take measures, point b) and paragraph (2) of Article 32 (1) and instructs, the Company that it has been documented within 30 days of this decision becoming final take appropriate technical and organizational measures to ensure that its data management operations should be in accordance with legal provisions.

The Authority states that by recording the health data of the guests, the Company violated Article 6 and Article 9 (2) of the GDPR, therefore the Authority prohibits in connection with appointments, the management of the health data of the guests and instructs the Company to immediately complete the appointments in its database the recording of health data during comments, and also instructs that this decision within 8 days of its becoming final, delete it in a documented way for the appointments among the comments made, the personal health data of the persons concerned.

The Authority states that since the Company handled the guests' data without a legal basis for marketing purposes, therefore violated Article 6 (1) of the GDPR in relation to this data management paragraph. For all these reasons, the Authority instructs the Company to make this decision final terminate illegal data processing and data processing within 30 days of the divorce bring the operation into line with the legal provisions by verifying the guests the legal basis for processing your data for marketing purposes.

6.

The Authority instructs the Company that within 8 days from the date of this decision becoming final as documented internally

delete the personal data processed through customer recommendation az

from its database.

7.

The Authority is the 1-4. the Company ex officio due to data protection violations specified in point

HUF 30,000,000, i.e. thirty million HUF

obligates you to pay a data protection fine.

The data protection fine shall be imposed by the Authority within 30 days of the date of this decision becoming final

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-2732-2/2023. FINE. number must be referred to.

1-6. the Company to take the measures prescribed in points from the receipt of this decision

must be submitted in writing within 30 days of the

certify to the Authority.

If the Company does not comply with its obligation to pay the fine within the deadline, a late fee will be charged

is obliged to pay. The amount of the late fee is the legal interest, which is the calendar interest affected by the delay

is the same as the central bank base rate valid on the first day of the semester.

1-6. non-fulfilment of obligations according to points, as well as the data protection fine and the late fee

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

No procedural costs were incurred in the procedure.

There is no place for an administrative appeal against this decision, but it is subject to notification

Within 30 days, it can be challenged in a public administrative lawsuit with a claim addressed to the Capital Court.

The statement of claim must be submitted electronically1 to the Authority, which will submit it together with the case

documents

forward to the court. The request to hold a hearing must be indicated in the statement of claim. The entire

for those who do not receive a personal tax exemption, the fee for the administrative lawsuit is HUF 30,000, the lawsuit

is subject to the right of material levy record. Legal representation is mandatory in proceedings before the Metropolitan Court.

The Authority shall post this decision on the Authority's website by indicating the identification data of the Company

publishes it.

I. Course of procedure, preliminary steps

I N D O C O L A S

Several reports were received by the Authority, in which the informants complained that a

Cameras at the company's headquarters, in every room (office, management, corridor, reception).

operates. According to reports, both the employees and the

guests are eavesdropped. Although the Company informs those concerned that a picture is being taken,

however, it does not provide information about the audio recording and the real purpose of the monitoring.

According to the announcements, the purpose of making the audio recording is to check the person performing the treatment

colleagues, as well as obtain information about guests and that the acquired

sell them even more treatments and facial care products based on information.

The reports received by the Authority also referred to the fact that the Company practices such recommendations

also continues, during which they ask their guests to enter the names of their acquaintances and

contact details, and then offer free treatment using this data

contacted stakeholders.

The Authority launched an official inspection in the case on October 19, 2021, and on October 20, 2021

held an on-site inspection at the beauty center located at the Company's headquarters.

(1)

(2)

(3)

(4)

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

can be filled out using a form-filling program (ÁNYK program). https://www.naih.hu/kozig-hatarozat-birosagi-felulvizsgalata

2

(5)

(6)

(7)

During the on-site inspection, the Authority became aware that the Company had misled its customers

its database is stored in the so-called “[…]” invoicing program system, therefore the Authority 2021.

on December 9, NAIH-7839-7/2021. addressed to […] Kft. with document no

(headquarters: [...]., hereinafter: […] Kft.) in order for the Company to send “[…]”

export of databases stored in software. [...] Kft. data export requested by the Authority

prepared and received by the Authority on December 21, 2021

he forgave

The Authority studied the Company's database, and then the findings of the on-site inspection, a

statements, as well as database analysis, decided to ex officio data protection

initiates official proceedings.

The Authority dated February 10, 2022, NAIH-2847-1/2022. notified the

Company that the provisions of the General Data Protection Regulation are presumed to be in violation

initiated a data protection official procedure ex officio. In its ruling, the Authority also

ordered a temporary measure, in which the camera data management was prohibited by the 2 pcs.

in the diagnostic examination room, the 10 pcs. in operator and the 5 pcs. in VIP operator and called the

Company to be certified by the temporary within 8 days of receipt of the order

performance of the measure.

(8) In addition to all this, in this order of the Authority, clarification is provided in order to clarify the facts

requested from the Company.

(9)

The Company is the Authority NAIH-2847-1/2022. he received his order with case number on February 14, 2022

at the company gate storage location, therefore the temporary measure until February 22, 2022, the Authority

you should have answered the questions clarifying the facts by March 1, 2022, the

However, the Company did not provide information on the issues contained in the Authority's order, and it

he also failed to certify the fulfillment of a temporary measure.

(10) The Authority decided to impose a procedural fine due to the above behavior, therefore NAIH-2847-2/2022. No. dated March 17, 2022, the Company was fined HUF 600,000 obliged to pay a fine and repeatedly called the Company to answer the questions.

(11) Since the Company did not comply with its obligation to pay fines, the Authority issued NAIH-2847-7/2022. ordered the procedural fine on September 7, 2022 with order no implementation.

(12) The Company is the Authority NAIH-2847-2/2022. 2022 in response to the questions asked in call no. responded on April 5 and stated that he complied with the temporary measure, which as proof, he attached a photo from the Company's server.

(13) Since the Company did not respond to the Authority's NAIH-2847-2/2022. repeated call no fully to the questions asked in the order containing, repeatedly with his conduct violated the CL of 2016 on the general administrative order. in § 6 of the Act (a hereinafter: Ákr.) and the cooperation and obligation to provide data, the Authority imposes an additional HUF 500,000 procedural fine decided in favor of, and NAIH-2847-8/2022. again on September 19, 2022 with order no called the Company to clarify the situation.

(14) The Company has NAIH-2847-8/2022. filed an action against his order no. and in the framework of immediate legal protection, he requested the ordering of suspensory effect. The administrative order in the case of his appeal, the court is conducting a simplified trial under case number 103.K.703.817/2022 away.

(15) The Authority NAIH-2847-8/2022. to the order of the Company on September 28, 2022 answered.

(16) Since in this answer the Company still did not confirm that it took over from Beauty and more Kft sent the information to 851 of its customers that as of June 1, 2021, the Company

continues to manage their personal data, and has not attached the camera

data management, as well as its legitimate interest in the management of customers' data for marketing purposes

nor its supporting interest assessment, the Authority NAIH-2847-11/2022. No. 5 October 2022

on the day of, he repeatedly called on the Company to clarify the facts.

(17) In this notice, the Authority also requested clarification from the Company regarding the fact that

newly attached, "Declaration", "Agreement" and "Contributors

"agreement and declaration" forms are filled out by whom and on what occasions and from when

is used by the Company, and what is the purpose and legal basis of photographs and video recordings

preparation, in connection with which they are filled out.

(18) The Authority NAIH-2847-11/2022. no., the Company on October 14, 2022

provided information in the document sent. This statement was made by the Company on October 18 –

beyond the deadline - he added, since, according to his claim, the Company is connected to camera data management

his interest assessment, made to support the priority of his legitimate interest, is the earlier one

was omitted from his statement due to a technical error. At that time, the Company attached the "weighing of interests

test at 1036 Budapest, Bécsi út 38-44. electronic operated in a beauty salon at no

for handling image recordings made by a surveillance system", dated October 14, 2022

document (hereinafter: interest assessment).

(19) As the Company explained in its statement of October 14, 2022 that Beauty and more Kft.

he cannot prove the delivery of letters sent to his customers to the Authority because

has changed mail system provider and therefore previous correspondence is not available to him,

on October 20, 2022, the Authority issued NAIH-2847-15/2022. with document no

Company's mail system provider, […] Kft. (headquarters: […], hereinafter:

Service Provider) to be sent to the Authority by the Company on June 1 and July 31, 2021.

a copy of the electronic letters sent with the address "Letter from the manager" between

Service provider performed on October 24, 2022.

(20) Since the Company's database did not contain any files related to it

data or information that any natural person would have contributed

management, and for the transfer of your data to other third parties, therefore the Authority

NAIH-2847-17/2022. no. dated November 16, 2022, again asked the Company,

to declare the manner in which it is recorded and recorded by the data subjects

contributions to data management for the purpose of direct business acquisition, as well as those concerned

regarding the management of your health data, and also explain the process of unsubscribing.

(21) The Company responded to the Authority's request on November 24, 2022. Then

the Authority informed the Company that in the official data protection procedure the evidence

procedure was completed and called that the evidence discovered during the clarification of the facts is

of the rules of document inspection

additional proof

can make motions. The Company received this notification from the Authority on December 7, 2022,

he did not comment on that.

by taking into account you can get to know and

II. It's true

II.1. Facts revealed during the official inspection

II.1.1. The Company's data processing with a camera

(22) The Company operates the Spandora Beauty Center at its headquarters (hereinafter:

Beauty Center), where in 2 diagnostic rooms and 15 treatment rooms facial and

they perform body treatments and medical aesthetic interventions. In addition, the Company

also distributes cosmetic products under the brand names "Deaura" and "Desheli".

(23) The Company is available on the website of the Company Information Service according to public, authoritative data

11/09/2017 was registered on, its main scope of activity is "physical

well-being improvement service". The Authority makes the Company's GDPR applicable during the procedure

examined his data management from the date after his divorce, but in order to clarify the facts

it also took into account the activities carried out in the previous period.

(24) During the on-site inspection on October 9, 2021, a total of 32 cameras were located at the site, the

2 cameras at the reception, 4 in the corridors, 1 at the back entrance, the two diagnostic

1 camera each in the room, 1 camera each in the 10 operators and 5 VIP operators, in the warehouse

1 camera, 1 camera each in the two customer service locations, 1 camera in the training room, the

2 cameras in the control office. The control office is a room consisting of a double room, the other of which

part also has 1 camera. Corporate events and meetings in the training room

are held, and many of the employees also spend their lunch break in this room.

In addition, there is 1 camera in the office of the labor manager and 1 in the so-called "interview"

in the room.

(25) The following areas were visible on the images of the cameras viewed on site:

- "t1ch1-t10ch10." in the image of the cameras in the operators, the cosmetic beds and beauticians

work area,

- in the image of cameras numbered "diag1ch11 and diag2ch12" the diagnostic rooms, including

desks and guest chairs so that the chairs are facing the cameras,

- in the image of the "VIP1ch5-VIP5ch9" cameras, the VIP operators with the cosmetic beds and

work areas,

- office workstations on the camera images "kontrollch13" and "kontrollch14",

- the entire training room in the "oktatoteremch10" picture,

- the labor office in the image of the "hrch15" camera

- the interview room on the "inter1ch16" camera image,

- the internal corridors on the image of the "corridor1ch11-corridor4ch14" cameras,

- the rear entrance door of the Beauty Salon in the image of the "hatsobejaratch15" camera,

- in the image of the "camera16" camera, the entire warehouse,

- "same service1ch1" and "same service2ch2" are the customer service rooms,

- the "recepcio1ch3" and "recepcio2ch4" cameras monitor the reception and the waiting room

yes.

(26) There was no data management information about camera surveillance at the reception. At the start of the inspection a

A representative of the authority found the server cabinet open, the cameras of the control rooms

could be viewed on the monitors in the room.

(27) The former IT specialist of the Beauty Center gave information over the phone that a

cameras can be accessed with the software called [...], which is on the computer desktop

employees can access it with a posted shortcut. Remove the recordings stored in the camera system

can be exported in AVI format. They can be downloaded by any user who [...] software

accesses the system using Examining the economic manager's computer, the […] software

could be opened, live images of the installed cameras were constantly visible on it, as well as 7

it was also possible to access 24-hour saved recordings going back to the day by downloading them.

(28) On the one hand, the employees are on the camera recordings saved by the Authority during the on-site inspection

workstations were visible, so that they could be seen and heard in each place

employees during work. On the image of the cameras placed in the operators, the cosmetic

beds are visible in their full extent, without covering, in such a way that on these beds the

during treatments, guests lie with their upper bodies covered with a bath towel. The cameras are a

operators also record sound.

(29) According to the statement of the Company's legal representative during the on-site inspection, the cameraman

The legal basis for data management is consent. In response to the Authority's question about what kind of information

the employees receive information about the data management with the cameras, the person staying at the site,

an employee in a senior economic position stated that verbal information upon entry

employees receive, there is no such information in the employment contract. THE

guests consent to data management by filling out and signing the consultation form, a

the following information statement on camera data management is included on the consultation sheet:

"I acknowledge that the Spandora Beauty Center is protecting me and the salon's employees

takes continuous camera recordings in the entire area of the salon, except for the washrooms and

the dressing rooms. With my signature, I certify that I have taken note of the camera recordings,

I agree to that and declare that I answered all questions honestly" statement as well

are signed.

(30) The Company on its website at this time in the "data protection policy" document only

fulfillment of contracts, contact and data processing for the purpose of acquiring business and making offers

name handled in connection with,

used

information provided by the Company on the management of information related to services

among the processed personal data, the image or voice of the data subjects is not mentioned, and there is no

it's about surveillance with a camera.

phone number, email data, and

Home address,

(31) The employee of the Company activates the sales manager machines in the presence of representatives of the Authority

state, which was done by entering the username of the given machine as a password,

i.e. the password is the same as the name of the user installed on the given machine. The username is a

it could be copied from a sheet of paper taped to the monitor. On one machine after logging in

the camera images monitoring the treatment rooms appeared on the home screen. The present

colleagues informed the representatives of the Authority that the person in the room

none of the machines have permanent users, colleagues are always sitting elsewhere.

(32) According to the statement made by the Company during the on-site inspection, the purpose of the camera surveillance is

the newer one

coordinating the work of therapists, as well as checking that the person performing the treatment

whether therapists communicate properly with guests and, if necessary, give based on this

give them instructions. Camera images are also available from other machines in other rooms, a

no observation record is made.

II.1.2. Management of the guest database

(33) According to the Company's statement, a consultation form is filled out with all guests at the reception desk who, but the telephone number and e-mail address are not recorded in all cases. If the guest does not purchases, the form will be destroyed within a few days. On-site with the Company telephone numbers were recorded on the back of the consultation sheet presented in the examination, which the provided information that recommendations.

(34) In response to the question asked on the consultation form, according to which you are interested in medical aesthetic intervention, the data of guests who answer yes are recorded in a separate excel table (name, age, phone number).

(35) The employees of the Company's call center record the telephone numbers in the excel tables in the so-called [...] into the system (hereinafter: database, guest database, guest register or software) and calls containing various campaigns and recommendations are launched from here. THE treatment times are also arranged with the guests through the call center.

II.2. Examination of the files of the requested database

(36) The […] IT software service containing the customer database is provided by […] Kft for, based on the contractual relationship with the Company since November 12, 2018.

(37) The earliest entry in the database files was created on October 20, 2010, but continuous entries were created in the database from May 4, 2015. In many cases

it can be observed that a significant amount of records were created at a given time. So for example 12/11/2018 34,992 with time 0:00:00, 15.05.2019. 4,975 at 13:04:28, while 2021.09.05. 208,076 new records were added at 0:00:00.

(38) The database consists of six files containing data belonging to the same topic: 1) basic data 2) partner characteristics 3) contracts 4) appointments 5) communication log 6) campaigns

(39) The "Basic data" file contains the basic data of the customers (name, possibly - mainly married in the case of clients – their short name, address, e-mail address, phone number, name of their therapist, on them

relevant notes, as well as the time when their data was entered into the Software

database). A total of 357,973 rows containing data with unique identifiers

(hereinafter: record) the database contains, of which 357,157 records can be considered as

relates to a natural person affected by data management.

(40) There are 2,218,913 entries in the "Partner characteristics" file. The on-site inspection

according to experience, under this menu item in the software, the guests' birth name, mother's name,

place and time of birth, identity document number, residential address card number are recorded,

also, the date of the last call, the outcome of the last campaign, the most recent are displayed here

reason for not being interested in the offer, and for sending the first contact message

date.

(41) The Authority has 2,490,999 communication records in the "communication log" file

identified. On the basis of this stock, it could also be established that the treatment of several guests and

the recording of related data was already started when the Company had not yet

was established, in this way, for example, the Company has a guest who first in 2015, then

They visited me by phone twice in 2018, and then again on June 2, 2020.

(42) […] Kft. stated in its response to the Authority on December 21, 2021,

that the data with the value "DEA migrated" is a so-called users

contain a label defined in terms of competence, which is not software provided by [...] Kft

standard predefined function. The software enables the Company to

supplement the used data model within your own authority, create unique labels with which

you can mark data records to facilitate later retrieval. It is at the request of the Company

in a separate column in data export

became

assigned the tag in question.

indicated for which data records

(43) In the "Contracts" file of the database, the day before the day of the establishment of the Company

1048 from the previous period. contract is included, which also indicates that by the Company

in the register kept, more than a thousand contracts have a validity beginning

when the Company did not exist.

(44) The Authority also compared the data of the "communication log" file with the contract

with the data of the persons having the "communication log" in the file

as a result of filtering, the database from the day of the foundation of the Company (September 11, 2017).

up to the date of its investigation, the Authority found 23,891 diary entries after the establishment, but

only 6,988 of the guests registered in this period had such a unique arrangement

with an identifier based on which it could be concluded that he has a contract with the Company

would be connected in connection with the provision or sale of services.

(45) In the column named "comment" of the "Records" file of the database, the Authority

found information about the guests that served as a reason to cancel the treatment, such as

for example, "her leg is operated on", "her daughter is sick", "her sugar has dropped", "she is pregnant". In the stock, for example, the

The term "patient" occurs 2,438 times, in addition, vaccination is mentioned in several columns,

as well as entries referring to vaccination from the first quarter of 2021.

III. Statements made by the Company during the official procedure

7

III.1. Statements related to camera data management

(46) According to the Company, the Company's managing director, HR manager, financial manager and

the storekeeper has access to it. The purpose of data processing with the camera is financial payments, as well as

checking values in handlers.

(47) Access to camera footage is subject to availability according to the Company's supplementary statement

from position. Thus, the recordings recorded by the cameras are taken by the Company's executive, as well as by the company

manager, for the purpose of complete control, he can use any financial, warehouse and other, a

to uncover problems related to the operation of the company, as well as potential customer complaints,
to clarify guest complaints. The financial manager of the Company is responsible for any financial issues
problems and matters related to money management, as well as for inventory control
has access to the recordings and the storekeeper can also check the recordings made in the warehouse. THE
In order to investigate potential employee complaints, the HR manager was given access to the
for a camera system.
(48) On April 5, 2022, the Company declared that camera data management
employees receive verbal information, and guests receive information on the consultation sheets
written information, which they accept with their signature, and at the same time add to the data management
they contribute
(49) On September 28, the Company stated that the operation of the camera system requires a
its legal basis is the legitimate interest of the Company.
(50) To substantiate the priority of its legitimate interest, the Company on October 14, 2022
prepared an interest assessment and sent it to the Authority. According to the attached document, a
The company uses the camera system to protect its assets, as well as possible guest complaints
operated in order to investigate it more effectively. The goal to be achieved is fundamental to the Company
it serves its economic interest, in addition to all this, it also stands in the interest of the guests, since it is
based on a consideration of interests, in the absence of the recording of the images, the investigation of customer complaints
they would not be able to implement it at an adequate level.
(51) As a result of the weighing of interests, according to the Company, its interests are balanced a
with the interests of employees and guests using the services of the beauty salon, since
the Company provides them with information on the essential circumstances of data management,
and the deletion of the image recordings, if in his opinion their handling is not justified.
Complaints to asset protection and guest complaints if the images are not recorded
according to the Company, the implementation of its investigation to a suitable standard is low a
probability. The executive, the financial manager, the labor manager and the storekeeper have access

despite the Authority's request, the Company did not justify the necessity of his right for each position

yes.

(52) According to the statement made by the Company on April 6, 2022, the recordings will be kept by the Company for 60

days

yes. On September 29, 2022, the Company amended this statement according to the

The 60-day retention period for camera images resulted from a wrong setting of the system, which

the Company brought it into line with the information on data management on its website, and for 3 days

changed it.

III.2. Statements regarding the management of the database

III.2.1. The source of the personal data in the database

(53) According to the Company's statement on April 5, 2022, with guests and potential

they communicate with customers via newsletters and by phone. With the phone calls

in connection with the September 28 statement, the Company explained that the marketing group

sends a list of Facebook applicants to the call center every day who have made an appointment

interested parties are approached for this purpose. The call center and the

The company's receptionists make arrangements by phone.

(54) The legal basis for the management of personal data used for direct business acquisition is for the guests

consent provided on the consultation form.

(55) On September 28, 2022, the Company attached newsletters and consultation sheets to the 2022

from 26 July to 30 August 2022 and stated that the consultation papers

they are destroyed every month, unless someone buys a product or service. THE

the personal data of guests purchasing products and services for direct business purposes a

According to the Company's statement at the time, it is handled based on the Company's legitimate interest.

(56) At that time, the Company also declared that the personal data in the database

exclusively from guests applying for advertisements placed on its website and Facebook page

are derived from. In the past, they actually collected contacts through referrals from their existing guests

also, however, on October 25, 2021, the Company's employees were informed that

the Company will terminate the request for guest recommendations, so the referral service is currently not working

system at the Company.

III.2.2. Management of guests' data for marketing purposes

(57) The Authority NAIH-2847-11/2022. on October 6, 2022, he asked the Company in document no

present it for data processing for marketing purposes

its legitimate interests take precedence

to support the assessment of interests, and also how it informs the affected parties

on the conditions of data management for marketing purposes.

lacing

(58) The Company replied that the Company does not use the buyers' data for marketing purposes

use. According to this statement of the company, data processing for marketing purposes is only for models

and in the case of employees, it is realized in such a way that the Company records the

to display its promotional offers, in which models and employees of the Company

are included. These advertising materials are displayed in advertisements and on social media platforms

Company. Models and employees can manage their personal data by a

Declaration/Declaration",

“Contributory Agreement and

declaration" by filling in forms.

"Agreement" and

(59) Contributions to these promotional videos showing the products

however, they are only ad hoc as they cover a total of four shooting days, so they are present

they cannot be evaluated from the point of view of the marketing activity examined in the procedure.

(60) A significant number of guests were created in the guest database prior to the founding of the Company

in relation to personal data, the Company explained that the DeAura Center is operated by Beauty and

more Kft., of which the Company is not the legal successor. Company 851 from Beauty and more Kft

received its main data on May 10, 2021. The contract transfer agreement and the

the Company sent the related guest list to the Authority, and also attached a

information letter, which he claimed to have sent to these guests. In these the

in the letters it was stated that Beauty and More Kft. completed the 1061 Budapest, Andrássy út 4.

activities carried out during and hands it over to the Company, which is located at 1036 Budapest Bécsi út 38-44.

in the Új Udvar Shopping Center located at no

booked treatments. Accordingly, payments must be made to the Company's account

to fulfill the following. If the guest does not agree with the above changes, he can request the

contract termination. The Company could not prove the sending of the letters to the Authority,

since, according to his claim, the Company changed its mail system service provider and therefore the previous one

correspondence is not available to him.

(61) Contact of the Authority by the Service Provider that previously operated the Company's mail system

based on a total of 7 e-mails sent during the examined period, as well as 5 e-mails given to

sent a reply email. Based on the submissions by the Service Provider and the Company, as well as from

that the mail system presumably stored only those letters for which it is

the data controller has received at least one reply message from the addressee, it can be

to conclude that probably many more customers - preferably all 851 - were informed by the

Company that instead of DeAura Center, the Company will continue to process their personal data

activities related to its management.

(62) Based on the correspondence submitted by the Company and attached by the Service Provider, no

information contrary to the Company's assertion that the data controller

informed all clients taken over from Beauty and more Kft. about the change in his person.

III.2.3. Management of guests' data for the purpose of sending newsletters

(63) By entering their name, email address and telephone number via the Company's website

applying guests can mark their wishes in a separate checkbox on the application form

to be informed about discounted offers, and subscribe to the Spandora newsletter.

(64) At the same time, when examining the Company's guest database, the Authority did not find the "partner

features" or in the "communication log" menus referring to subscribing to the newsletter

registration, so he contacted the Company, who replied that the consent statements

the Company stores it on a paper basis in the consultation sheets. The consultation sheets are provided by the Company

store in a lockable cabinet. This statement contradicts the Company's on-site

with his statement during the inspection, according to which the consultation sheets will be destroyed.

However, given that the fact of destruction was not verified, the Authority a

accepted the storage of consultation sheets as real.

(65) Unsubscribing from the newsletter is according to the latest statement of the Company at the bottom of the sent

newsletters

by clicking on the "unsubscribe" link. The Company keeps a table of unsubscribers, which

sent to the Authority.

III.2.4. Management of health data

(66) In the Company's database, in the "remarks" column of the "appointments" file, with illness,

records data related to pregnancy and coronavirus vaccination. Company statement

according to them, these data are processed because they cannot perform the treatment on patients, but it is

the guests do not lose an appointment. Conversely, if a guest does not show up for the treatment

and does not indicate the reason for his absence, then the treatment can be considered used.

(67) The consultation data sheets may also contain information on the health status of the guests

data, if herpes, allergy, pregnancy, surgical intervention are indicated

columns.

(68) In response to the Authority's question, the Company stated that the health data of the affected persons is

it is managed on the basis of the consent of those concerned, which, according to the Company, is the consultation data sheet

signed by the guests concerned.

ARC. Applied legal regulations

According to Article 4, Point 1 of the General Data Protection Regulation, "personal data: the identified or

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 such as a name,

number, location data, online identifier or physical, physiological, genetic,

on the basis of one or more factors relating to his intellectual, economic, cultural or social identity

identifiable."

According to Article 4, point 11 of the General Data Protection Regulation, "consent of the data subject": the data subject

a voluntary, concrete and well-informed and clear declaration of his will, with which

indicates by the relevant statement or by an act clearly expressing the affirmation that

gives his consent to the processing of his personal data.

According to Article 5 (1) 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

("legality, due process and transparency");

b) should only be collected for specific, clear and legitimate purposes, and should not be treated with them

in a manner inconsistent with the objectives; in accordance with Article 89 (1) does not qualify as such

incompatible with the original purpose for the purpose of archiving in the public interest, scientific and historical

further data processing for research or statistical purposes ("target binding");

c) they must be appropriate and relevant in terms of the purposes of data management, and as necessary

they must be limited ("data sparing");

d) they must be accurate and, if necessary, up-to-date; all reasonable measures must be taken

in order to provide inaccurate personal data for the purposes of data management

be deleted or corrected immediately ("accuracy");

e) must be stored in such a way that only personal data can be used to identify the data subjects

allows for the time necessary to achieve its treatment goals; personal data for a longer period of time

may only be stored if personal data is processed in accordance with Article 89 (1)
for the purpose of archiving in the public interest, or for scientific and historical research purposes, in accordance with
paragraph
will take place for statistical purposes, the protection of the rights and freedoms of the persons concerned in this regulation
taking into account the implementation of appropriate technical and organizational measures prescribed for
("limited shelf life");
f) must be handled in such a way that appropriate technical or organizational measures
the appropriate security of personal data should be ensured with its application, or the data is unauthorized
against illegal handling, accidental loss, destruction or damage
including protection ("integrity and confidentiality").
According to paragraph (2), the data controller is responsible for compliance with paragraph (1), and is also able
there must be evidence of this compliance ("accountability").
Pursuant to Article 6 of the General Data Protection Regulation, personal data are only processed when
and legal insofar as at least one of the following is met:
a) the data subject has given his consent to the processing of his personal data for one or more specific purposes;
b) data processing is necessary for the performance of a contract in which the data subject is one of the parties
necessary to take steps at the request of the data subject prior to the conclusion of the contract;
c) data management is necessary to fulfill the legal obligation of the data controller;
d) data management is to protect the vital interests of the data subject or another natural person
necessary due to;
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 is necessary to enforce the legitimate interests of the data controller or a third party,
unless such interests or fundamental rights of the data subject take precedence over these interests
and freedoms that require the protection of personal data, especially if the data subject
child.

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

for data management.

According to Article 7 (1) of the General Data Protection Regulation, if data management is based on consent,

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

contributed to its treatment.

Based on Article 12 (1) of the General Data Protection Regulation, the data controller is compliant

takes measures in order to allow the data subject to process personal data

all relevant information referred to in Articles 13 and 14 and Articles 15-22 and everything according to Article 34

certain information in a concise, transparent, understandable and easily accessible form, clearly and

provide it in plain language, especially for any information addressed to children.

The information must be provided in writing or in another way, including, where applicable, the electronic way.

Verbal information can also be provided at the request of the data subject, provided that the data subject has confirmed

otherwise

identity.

Paragraphs (1)-(2) of Article 14 of the General Data Protection Regulation:

(1) If the personal data was not obtained from the data subject, the data controller shall make it available to the data subject

releases the following information:

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) categories of personal data concerned;

e) recipients of personal data, or categories of recipients, if any;

f) where applicable, the fact that the data controller is a recipient from a third country or a

wishes to forward the personal data to an international organization, as well as the Commission

the existence or absence of a conformity decision, or in Article 46, Article 47 or Article 49

In the case of data transfer referred to in the second subparagraph of paragraph (1), the appropriate and suitable indication of guarantees, as well as the methods for obtaining a copy of them or that reference to their contact information.

(2) In addition to the information mentioned in paragraph (1), the data controller makes available to the data subject the the following supplement necessary to ensure fair and transparent data management for the data subject information:

a) the period of storage of personal data, or if this is not possible, this period aspects of its definition;

b) if the data management is based on point f) of paragraph 1 of Article 6, the data controller or a third party is entitled about your interests;

c) the data subject's right to request access to the personal data relating to him from the data controller access, their correction, deletion or restriction of processing, and the personal may object against the processing of data, as well as the data subject's right to data portability;

d) data management based on point a) of Article 6 (1) or point a) of Article 9 (2) the right to withdraw consent at any time, which does not affect the the legality of data processing carried out on the basis of consent prior to withdrawal;

e) the right to submit a complaint addressed to a supervisory authority;

f) the source of the personal data and, where appropriate, whether the data is from publicly available sources whether they originate; and

g) the fact of automated decision-making referred to in paragraphs (1) and (4) of Article 22, including profiling as well as, at least in these cases, the applied logic and its comprehensibility information about the importance of such data management and what can be expected for the data subject has consequences.

Based on Article 24 of the General Data Protection Regulation (1) The data controller is responsible for the nature and scope of data management, its circumstances and purposes, as well as the implications for the rights and freedoms of natural persons, vary

appropriate technical and organizational, taking into account the probability and severity of the risk

implements measures to ensure and prove that the processing of personal data

is done in accordance with this regulation. These measures are reviewed by the data controller and are necessary

updates it if necessary.

(2) If it is proportionate in relation to the data management activity, referred to in paragraph (1).

as part of the measures, the data manager also applies appropriate internal data protection rules.

Based on built-in and default data protection according to Article 25 of the General Data Protection Regulation (1)

the data controller is the state of science and technology and the costs of implementation, as well as data management

nature, scope, circumstances and purposes, as well as the rights and freedoms of natural persons

all data management, taking into account the reported risk of variable probability and severity

when determining the method, as well as during the data management as appropriate technical and organizational

implements measures - for example, pseudonymisation - which are aimed at, on the one hand, data protection principles, e.g

the effective implementation of data saving, on the other hand, the requirements contained in this regulation

data management is the incorporation of guarantees necessary for its fulfillment and the protection of the rights of the data

subjects

into the process.

(2) The data controller implements appropriate technical and organizational measures to ensure that

by default, only personal data that is specific should be processed

obsession

data

accidental

personal

from its unlawful destruction,

they are necessary from the point of view of a specific data management purpose. This obligation applies to collected personal

for the amount of data, the extent of their processing, the duration of their storage and their accessibility. These are it

measures must in particular ensure that personal data by default a

without the intervention of a natural person, an unspecified number may not become accessible

for a person.

According to Article 32 (1) point b) of the General Data Protection Regulation, the data controller and

data processor, the state of science and technology and the costs of implementation, as well as data management

nature, scope, circumstances and purposes, as well as the rights and freedoms of natural persons

taking into account the reported risk of varying probability and severity, appropriate technical and

implements organizational measures to ensure that the level of risk is appropriate

guarantees data security, including, among others, where applicable:

b) the ongoing confidentiality of the systems and services used to manage personal data

its security, integrity, availability and resilience;

(2) When determining the appropriate level of security, the

risks arising from data management, which are especially transmitted, stored or otherwise

handled

from losing

alteration, unauthorized disclosure or the unauthorized access to them

they arise from access.

According to Section 9 (2) of Act I of 2012 on the Labor Code (hereinafter: Act): A

an employee's right to privacy can be restricted if the restriction is based on the purpose of the employment relationship

it is absolutely necessary for a directly related reason and proportional to the achievement of the goal. The right to privacy

the manner, conditions and expected duration of its restriction, as well as its necessity and proportionality

the employee must be informed in writing in advance of supporting circumstances.

Mt. 11/A. Based on paragraph (1) of § The behavior of the employee related to the employment relationship

can be checked among Within this framework, the employer can also use a technical device, as per

informs the employee in advance in writing.

Infotv. According to Section 60 (1) in order to assert the right to the protection of personal data

the Authority may initiate official data protection proceedings ex officio.

Infotv. 60/A. According to paragraph (1) of §

one hundred and fifty days, which does not include the communication of the data necessary to clarify the facts

the time from the invitation to its fulfillment.

Infotv. According to § 61, paragraph (1), point a) in the decision made in the data protection official procedure

the Authority is Infotv. In connection with the data management operations specified in § 2, paragraph (2), the

may apply the legal consequences specified in the general data protection regulation.

Infotv. According to paragraph (2) of § 61, the Authority may order in its decision - the data controller or the

disclosure by publishing the identification data of the data processor, if the decision

affects a wide range of persons, it was brought in connection with the activities of a body performing a public task, or

the severity of the infringement justifies disclosure.

Infotv. 75/A. §: The Authority is contained in paragraphs (2)-(6) of Article 83 of the General Data Protection Regulation

exercises its powers taking into account the principle of proportionality, especially with the fact that the personal

regarding data management - in legislation or in a mandatory legal act of the European Union

in the case of the first violation of specified regulations, to remedy the violation - that

in accordance with Article 58 of the General Data Protection Regulation - you are primarily the data controller

takes action with a warning from the data processor.

Article 58 (2) b), d), i) and g) of the General Data Protection Regulation: The supervisory authority

acting in its corrective capacity:

b) condemns the data manager or the data processor if his data management activities violated e

the provisions of the decree;

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

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

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

or deletion, or limitation of data management, as well as Article 17 (2) and Article 19

properly orders the notification of the recipients with whom or with whom it is personal

data were reported.

All supervisory authorities based on Article 83 (1) of the General Data Protection Regulation

ensures that due to the violation mentioned in paragraphs (4), (5), (6) of this regulation, based on this article

imposed administrative fines are effective, proportionate and dissuasive in each case

to be

According to Article 83 (2) of the General Data Protection Regulation, administrative fines are applicable on a case-by-case

basis

depending on the circumstances of Article 58(2) a)-h) and j) of the General Data Protection Regulation

must be imposed in addition to or instead of the measures mentioned in When deciding whether it is necessary

whether there is an administrative fine to be imposed, or when determining the amount of the administrative fine

in each case due consideration shall be given to the following:

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

its scope or purpose, as well as the number of persons affected by the infringement, as well as the damages suffered by them

extent of damage;

b) the intentional or negligent nature of the infringement;

c) on the part of the data controller or data processor in order to alleviate the damage suffered by the data subjects

any action taken;

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

technical and organizational measures implemented on the basis of Articles 25 and 32 of the Data Protection Regulation;

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

f) remedying the violation with the supervisory authority and mitigating any negative effects of the violation

extent of cooperation for;

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, in what detail;

i) if against the relevant data manager or data processor previously - in the same matter -

the measures referred to in Article 58 (2) of the General Data Protection Regulation were ordered

one of them, compliance with the measures in question;

j) whether the data manager or the data processor complied with Article 40 of the General Data Protection Regulation.

for approved codes of conduct according to Article or according to Article 42 of the General Data Protection Regulation

for approved certification mechanisms; 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.

According to Article 83 (5) of the General Data Protection Regulation, violation of the following provisions –

in accordance with paragraph (2) - with a maximum administrative fine of EUR 20,000,000, or

in the case of enterprises, representing no more than 4% of the total annual world market turnover of the previous financial

year

amount, with the higher of the two amounts being imposed:

a) the principles of data management - including the conditions of consent - Articles 5, 6, 7 of the General Data Protection

Regulation

and in accordance with Article 9;

b) the rights of the data subjects are set out in Articles 12-22 of the General Data Protection Regulation. in accordance with

Article;

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

44-49 of the General Data Protection Regulation. in accordance with Article;

d) IX of the general data protection regulation. obligations according to the law of the Member States adopted on the basis of

chapter;

e) the instructions of the supervisory authority according to Article 58 (2) of the General Data Protection Regulation,

and for the temporary or permanent limitation of data processing or the suspension of data flow

non-compliance with the relevant notice or Article 58 (1) of the General Data Protection Regulation

in violation of the failure to provide access.

14

Decision of the Authority

Infotv. Based on subsection (2) of § 61, the Authority may order that the data controller, or the

- disclosure by publishing the identification data of the data processor, if

a) the decision affects a wide range of persons,

c) the severity of the infringement justifies disclosure.

V.

V.1. Data management with a camera

V.1.1. General comments

(69) The Company operated a camera system consisting of 32 cameras in the area of the Beauty Center. THE

cameras in the warehouse, reception, corridors, back entrance, customer service

rooms, offices, as well as in diagnostic rooms and operating rooms, images are taken

and audio recordings.

(70) Image and voice of the data subject based on Article 4 (1) of the General Data Protection Regulation

is considered personal data. The identified or identifiable natural person is affected.

Pursuant to all of this, if a natural person can be identified based on a recording,

then the created image or sound recording is personal data, the making of the recording

is considered data management.

(71) The data processing carried out by the Company is affected by the Company's employees and guests.

(72) During the on-site inspection, the Authority examined the images of each camera separately and

found that based on the quality of the video and audio recordings by the camera surveillance

affected persons can be identified in the recording. The Company, on the one hand, in such premises

operates the cameras where the employees work, thus to the employees' workstations

and the cameras in the operators and training rooms

during work, and in the control room during meals, in operators and

and in customer service rooms, in addition to employees, guests are also continuously served
keeps him under observation in such a way that during the treatments he is often in incomplete clothing
are visible.

(73) According to the Company's statement, for the admissions, the managing director, the financial manager, a
the labor manager and the storekeeper have access. According to what was experienced during the on-site inspection
however, the camera images are also seen by the sales manager, as he says the recordings
based on checks that the person performing the treatment
do therapists communicate properly a
with guests.

(74) The Company does not have a regulation on camera data management.

V.2. Defining the goals of camera data management in general

(75) According to the information on the consultation sheets, the guests and the salon are monitored
is done for the protection of its employees. The official data protection procedure by the Company
on the other hand, in the amended data management information after its launch, the cameraman
the purpose of monitoring is to improve the service and check the work of the employees. THE
In the statement made by the company in the official data protection procedure, the development of the service and the
employees monitoring goals supplemented the possible complaints effective
response and asset protection with goals. Finally, in his consideration of interests on this
referred to data management purposes.

(76) Targeted data management according to Article 5 (1) point b) of the General Data Protection Regulation
personal data only for specific, clear and legitimate purposes
can be collected, and it is forbidden to handle it in a way that is incompatible with the specified goals.

The data management goals must be defined in detail and precisely before the start of monitoring
to determine. If a data controller performs monitoring for several data management purposes, a
in relation to the camera, per purpose

monitoring purposes in each use

must be documented, otherwise data management will not

transparency meets

neither of his requirements.

(77) The European Data Protection Board on the handling of personal data using video devices

3/2019. According to point 19 of the guideline no. (hereinafter: Guidelines), for example, a

asset protection, enabling subsequent proof in connection with possible damage events

is considered a legitimate data management purpose in general, but this alone is not sufficient

to the legality of data management, namely in order for the legitimate interest to really exist, a

before the actual start of monitoring, an actual emergency situation must arise which

it can be, for example, a damage event or incident that actually occurred previously.

(78) The Company did not clearly define the purpose of the camera operator's data management, since the data subjects

the goals indicated on the consultation sheets and provided on the Company's website

the goals described in its information are not consistent with each other and do not match

nor with the statements made by the Company to the Authority during the procedure.

(79) Furthermore, the Company on the spot, as well as in its declarations and consideration of interests only

referred to the various data management purposes in general and did not explain them in any of them

in detail, in each room, with which cameras, specifically which of the four

performs the monitoring for data management purposes. Based on all of this, the Authority concludes that a

The company violated Article 5 (1) point b) of the General Data Protection Regulation

the principle of purpose-bound data management, as well as stated in point a) of Article 5 (1).

the requirement of transparent data management.

V.3. Monitoring of employees

V.3.1. The purpose of monitoring employees

(80) In the Beauty Salon at the reception, in the corridors, in the operators, in addition to providing the service,

in control rooms often used by employees for rest and meals, as well as a

cameras were installed in the warehouse and at the back entrance. The Company's employees in this way

in each room during work, as well as during their rest time

monitored by the camera system.

(81) In relation to the camera surveillance used in the workplace, the starting point is Mt.

according to Article 42, paragraph (2), point a), the employee is the employee based on the employment contract

is obliged to perform work under the direction of the employer. In accordance with this, the legislature in Mt.

It was defined as the basic duty of the employee in points b) and c) of Section 52 (1).

that the employee is obliged to be available to the employer during his working hours and his work

with the generally expected expertise and care, the rules applicable to your work,

perform according to regulations, instructions and customs. To comply with these legal obligations

the legislator in Mt. 11/A. Section (1) provides the opportunity for the employer to a

check the employee's behavior related to the employment relationship, whether technical

also by using a tool. This right may involve the processing of personal data.

(82) Section 9. (2) of the Mt. further states that the employee's personal right

may be restricted if the restriction is for a reason directly related to the purpose of the employment relationship

absolutely necessary and proportional to the achievement of the goal. On the method of limiting the right to privacy,

conditions and expected duration, as well as supporting its necessity and proportionality

circumstances, the employee must be informed in writing in advance.

(83) In case of monitoring for the purpose of property protection, the employer must prove that in fact

there are circumstances that justify the placement of individual cameras and others

way, the goal to be achieved cannot be ensured. It is also important in the case of property protection monitoring

requirement that the employer must pay special attention to the fact that the given camera

his point of view should basically be focused on the asset to be protected and should not be based on the above

into a tool suitable for monitoring the work of employees.

(84) According to the above, an acceptable data protection goal of asset protection in the warehouse may be

regarding data management and the camera directed to the corridors and the rear entrance door

asset protection can also be considered a suitable data management purpose. However, the Authority does not recognize it

the asset protection goal is legitimate in relation to the offices, managers and control rooms, since

on the one hand, the Company did not verify the assets to be protected in these premises

are located, nor any other installation of cameras for property protection purposes

did not indicate a reason supporting its necessity for these premises. Besides that

surveillance in these rooms is not even a proportionate measure, since the corridors and

exit cameras, as well as keeping the doors of the rooms closed, as well as in the operators

documenting the use of tools and machines located provide adequate protection a

against misappropriation of assets. In the absence of assets to be protected, it is also disproportionate

neither is the continuous monitoring of the training room used by employees for meals.

(85) Investigating guest complaints as efficiently as possible, improving the service as a data management service

regarding the purpose, the Authority also did not find it justified that the employees

monitoring would be a necessary measure to achieve this goal, since the Company

did not present a single specific case where the investigation of guest complaints and the

in order to improve services, the camera recordings would have been necessary, and a

According to the authority's point of view, the use of camera footage is not even suitable for achieving the goal

device.

(86) According to the Company's statement and its published information on data management, it is operated by it

cameras are also used to monitor employees. During the on-site inspection, the Company also

submitted that the video and audio recordings are used so that the sales staff

check the proper communication and sales of new employees with customers

behavior and, if necessary, they can coordinate sales with instructions.

(87) Mt. 11/A. Based on § (1), the employer may check the employee a

in connection with an employment relationship, even with a technical device, but in writing in advance

– also covering information according to Article 13 (1)-(2) of the General Data Protection Regulation

– you must inform the employee, avoiding that the cameras become a secret surveillance tool

divorce.

(88) The Constitutional Court 36/2005. stated in its decision no. that "by electronic means

monitoring is capable of intruding into the private sphere, intimate (sensitive)

record life situations even in such a way that the person concerned does not even know about the recording or does not have

it

in a position to consider the admissibility of such recordings and those

consequences. The surveillance carried out in this way goes beyond the violation of the right to privacy - it is broader

and in a deeper sense - it can affect the right to human dignity in general. The private sector

its essential conceptual element is precisely that, against the will of the person concerned, others cannot penetrate there

in, or not be allowed to look in at all. If the unwanted insight does happen, not only that

the right to privacy in itself, but other things that fall within the scope of human dignity

authorization elements, such as for freedom of self-determination or physical-personal integrity

real rights may also be violated."

(89) Cameras according to the above are permanent for employees and their activities

It cannot be operated for observation without a specific purpose, and it is also illegal

can also be considered the use of an electronic monitoring system whose purpose is to

influencing the workplace behavior of employees. You can't have such cameras

operate without a purpose or for a purpose that is not clearly defined, exclusively a

employees and their activities are observed. Such are the exception

workplaces where the life and physical integrity of employees may be in direct danger, thus

an exceptionally operable camera in, for example, an assembly hall, a smelter, or an industrial plant

in other facilities containing a source of danger. However, it must be emphasized that - it is

Also following the practice of the Constitutional Court - the camera can only be operated in that case

in order to protect the life and physical integrity of employees, if the danger actually exists and

immediate, i.e. potential danger cannot be a constitutionally acceptable data management goal.

(90) The teaching of sales activities is different from observing and recording treatments, a

using methods that avoid handling the personal data of guests and employees, for example

it could also be implemented with trainings, therefore the image of the guests and employees and

regarding the treatment of his voice, the Authority does not consider the necessity and

maintaining proportionality requirements.

(91) On the basis of the above, the aimless, continuous monitoring of employees is carried out by a

Authority did not accept it as a legitimate data management purpose and therefore found that a

monitoring of employees does not comply with Article 5 (1) of the General Data Protection Regulation

of the principle of purpose-bound data management according to paragraph c).

V.3.2. The legal basis for monitoring employees

(92) In relation to electronic monitoring systems used in the workplace, the general

Compliance with the basic principles of the Data Protection Regulation is extremely important for the employer

camera data management established by should be legal.

(93) According to the Company's on-site inspection and statements of April 5, 2022, data management is

was based on the consent of those concerned, and then the Company supplemented this on September 28, 2022

with the legal basis of legitimate interest by referring to both legal grounds at the same time.

(94) As a legal basis for consent according to Article 6 (1) point a) of the General Data Protection Regulation

it can be properly referred to if its conditions are met. To the contribution

according to the definition according to the general data protection regulation, it must be provided with appropriate information

it must be based on, be voluntary, and the consent of the person concerned

concretely, unambiguously, a statement or act of unmistakably expressing confirmation

must be declared via

(95) Both the Mt. and the general data protection regulation require that the data subjects be informed

(96)

established Data Protection Working Group3

about the circumstances related to data management.

Furthermore, consent must be voluntary. Regarding the voluntary contribution

at the same time, the data protection directive in force before the general data protection regulation2 29.

according to article

hereinafter: Data protection

Working Group) explained in several resolutions that in the employee-employer relationship

the possibility of voluntary contribution can be questioned, it is basically only possible then

to refer when it is clear that unconditional "advantages" are obtained during data management

employee, and cannot suffer any disadvantages in case of refusal of data processing. THE

in the world of work - as in the present case - instead of the consent of the person concerned, there is therefore a different

legal basis, a

the use of data management based on the employer's legitimate interests is justified. The Company has this legal basis

referred to after the initiation of the procedure, and then prepared and submitted a consideration

To authority.

(the

2 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free flow of such data

European Parliament and Council Directive

3 The Data Protection Working Group, prior to the start date of the application of the general data protection regulation, with

data protection,

and was an independent European advisory body dealing with issues related to the protection of privacy, replaced by the

European

The Data Protection Board stepped in.

18

(97) According to the Guidelines, consent can only be used in exceptional cases

as a legal basis, while in practice the reference to legitimate interest is one of the most common

occurring and appropriate legal basis.

(98) During the procedure, the Company amended its position and information and both

contribution, both the

as its legal basis. One

data processing can have one legal basis at the same time, since the simultaneous application of several legal grounds

may violate the principles of transparency and fairness. For this reason, it cannot be accepted that the cameraman

the Company assigned two different legal bases for monitoring in parallel.

legitimate interest has been indicated by the data management

(99) The assessment of interests made afterwards, during the procedure, does not retroactively prove a legal basis,

however, the Authority also examined the existence of this legal basis.

(100) In order for data processing based on legitimate interest through camera surveillance to be legal

data processing should be proportionate to the goal to be achieved and necessary to achieve the goal

There has to be.

(101) In view of the principle of data saving, the data controller must first thoroughly

examine whether the measure is suitable for achieving the set goal and, secondly, whether it is appropriate

and whether it is necessary for the objectives to be achieved. Before putting a camera system into operation, set it up as well

it is necessary to measure where and when video surveillance measures are absolutely necessary,

furthermore, in order to achieve the specified goals, there is an equally effective protection

an insurance measure that less impairs the rights of those concerned.

(102) In its assessment of interests, the Company does not explain separately that a

the rights and freedoms of data subjects in different types of premises

does it limit proportionally. Based on all of this, the data management goals that the Company wants to achieve

in order to achieve this, continuous recording of the work is not considered necessary,

nor proportionate data management.

(103) A

above

in addition, based on recital (47) of the GDPR, data management

during its planning and implementation, the reasonable expectations of the stakeholders must also be taken into account. An employee at work usually does not expect his employer to observe,

furthermore, the Company in the area of the Beauty Center not only in the warehouse, but also in the operators, a it also operates cameras in control offices and in the training room, where it is also unreasonable to expect observation.

(104) Considering that the Company was unable to prove that the employees were monitored by cameras would have a legal basis for its continuous monitoring for the purposes it indicated, as neither the there is no legal basis for consent or legitimate interest. By doing so, the Company violated the Article 6 (1) of the General Data Protection Regulation.

V.3.3. Informing employees about camera data management

(105) In the case of data management through a camera system, the data controller is the personal data is collected from the data subject, therefore the obligation to provide information according to Article 13 of the GDPR is sufficient

to the data controller. Mt. also stipulates that the affected parties must be informed about circumstances related to data management. Mt. 11/A. formulated in paragraph (1) of § general information obligation regarding the handling of personal data is general it must also be fulfilled taking into account the provisions of the data protection decree, i.e. the general one is filled with content by the data protection decree, defining the circumstances under which e regarding this, the employer must inform the employees in advance in writing.

(106) From the principle of accountability according to Article 5 (2) of the General Data Protection Regulation as follows, as well as on the basis of Article 12 (1), the information to the controller is concise, in a transparent, comprehensible and easily accessible form, formulated in a clear and understandable way must provide, in writing or in another way - including, where applicable, the electronic way. The z

also from the principle of accountability according to Article 5 (2) of the General Data Protection Regulation as follows - the data controller, the employer must prove and certify the appropriate

the occurrence of prior information.

(107) According to the Company's statements, the employees talk about camera data management, and that they receive information through a data management information sheet.

(108) The Company has a data management policy in effect in the period prior to the official data protection procedure its information did not include the section on camera surveillance. The data management during the information procedure, in the updated version of the Company's website for data management inserted a paragraph among the relevant rules, according to which: "there is a camera in the salon monitoring works, the purpose of which is to improve the Company's services and the employees control of his work". In addition, the floor plan of the beauty salon is shown in JPEG format in the document on which the location of the cameras is marked with an X. The picture due to its small size, the location of the cameras is barely visible, so this information is not suitable for so that the employees concerned can identify the location and angle of view of the cameras.

(109) Regarding the prospectus, the Authority found that it does not meet the general requirements the requirements prescribed by the data protection decree, as it does not provide information on the individual about the placement of cameras and their purpose, the area they monitor, about the subject, or whether direct or recorded observation is carried out with the given camera employer. The information also does not provide for the specific duration of storage of the recording, about the rules for viewing the recordings, as well as about the type of the recordings purpose can be used by the employer.

(110) Regarding the possible oral information, the Authority further notes that no its content is proven and whether it happened.

(111) Based on all of this, the Authority concludes that the Company has violated Article 13 (1) of the GDPR-(2), since he incorrectly or misleadingly, incompletely informed the employees a about the management of their personal data.

V.4. Monitoring guests with a camera

V.4.1. The purpose of monitoring guests

(112) The Company mentions camera surveillance in its consultation data sheet and data management information
in connection with this, he indicated different goals, as in one the guests and the employees
protection, while in the other, the development of the service and the control of the work of the employees
appears, which is later followed by the effective response to possible guest complaints and the
In its statement of September 28, 2022, the Company also added asset protection goals.

(113) Since, as explained earlier, the Company did not clearly define the
camera data management purpose and did not explain in detail which rooms
with cameras, specifically for which data management purpose it monitors the data subjects, it can be said that
that the Company also violated the general data protection regulation in relation to guests
the principle of purpose-bound data management according to Article 5 (1) point b), and Article 5 (1)
the requirement of transparency according to paragraph a).

V.4.2. Informing guests about camera surveillance

(114) In order for the data management to be legal, an essential condition is that the data controller
provide adequate information. The relevant rules are the general data protection
contained in Article 13 (1)-(2) of the Decree.

(115) As part of the preliminary information, the data controller must strive to ensure that the data subject as much as possible
get a more complete and comprehensive picture of the management of your personal data, since the data subject can only
in this way, you have the opportunity to assess the impact of a specific data management on
to his private sphere. Paragraphs (1)-(2) of Article 13 of the General Data Protection Regulation contain
that the data controllers must inform about the minimum data management conditions
affected persons, however, this does not limit the fact that the data controller can be more accurate than this
provide information.

(116) In the case of camera surveillance, preliminary information is provided to the observed as a first step
must be provided when entering the area. At that time, outside the monitored area (at the entrance door,
at the gate) brief information provided by means of a pictogram is necessary and at the same time sufficient,

which, at the same time, must necessarily be supplemented as a second step by at least a

full (longer and detailed) information available on site.

(117) The first brief information, i.e. the pictogram, usually needs the most important information

contain about data management, such as the purposes of data management, the identity of the data controller and the

detailed information on the existence of the rights concerned. In addition, the more detailed,

for second-level information, as well as the place and method of its availability.

(118) Information on the availability of the latter information must therefore be provided on the displayed "pictogram"

(one of its functions is actually just this: data management cannot be avoided when entering the area

warns and refers to the possibility and accessibility of the necessary comprehensive information), and

this information must be made available at the request of the data subject. The second level

information must already include Article 13 (1)-(2) of the General Data Protection Regulation

all mandatory information related to data management.

(119) During the on-site inspection, the Authority established that it was not in the area of the Beauty Salon

posted information that the room is monitored by cameras. The company

in relation to its data management information, it has already been established above that it does not comply

and the requirements according to Article 13 of the General Data Protection Regulation.

(120) One-sentence information is indicated on the consultation data sheets, according to which "Spandora

The beauty center takes continuous camera recordings in the entire area of the salon (except for

washrooms and changing rooms)", is also not considered to be sufficiently detailed information.

(121) As a result of all this, the Company also violated the provision of information to the guests

Paragraphs (1)-(2) of Article 13 GDPR

V.4.3. The legal basis for monitoring guests

(122) Based on the Company's first statements and the attached documents, the guests are consulted

by signing the form, they acknowledge and at the same time agree to the fact that the Company is about them

makes continuous camera recordings.

(123) Consent must be based on information, because information is essential

it is a condition for those concerned to be able to understand what they are agreeing to. If it is
the data controller does not provide adequate information, the disposition of the data subjects over their data
it will only be apparent.

(124) In the case of continuous monitoring, the consent of those concerned can only serve exceptionally
as a legal basis, since the conditions according to Article 7 of the General Data Protection Regulation only then
are fulfilled if the data controller can prove that everyone involved is already using the camera
gave their consent to data management before entering the monitored area,
furthermore, if the data subject withdraws his consent, the data manager will have difficulty
can prove that it no longer handles personal data.

(125) Pursuant to the above, since the Company is neither on the consultation pages nor in the Beauty Salon
is not available to guests in its territory or in its data management information
information, the consent is considered an invalid legal basis.

(126) In the document attached on October 18, 2022, the Company later stated that the
camera system is also operated based on the Company's legitimate interest, but the guests are personal
the Company did not carry out a separate assessment in connection with your data and thus it was not charged
as proof that the cameraman is in the actual, legitimate interest of the Company
use observation to achieve the goals defined above. The Company also does not
nor did it prove that the measure was necessary to achieve these goals.

(127) According to the Guidelines, the legitimate interest is also considered to be truly existing and actually existing
must be, it cannot be theoretical at the time of data processing, as it is
Court of Justice of the European Union C-708/18. he also stated in point 44 of his judgment in case no.

(128) According to the Guidelines, the data controllers carried out to establish the existence of a legitimate interest
during the investigation, the reasonable expectations of the data subjects must be taken into account
at the time of treatment and in connection with it. Not the reasonable expectations of those involved
subjectively, but must be determined according to the fact that an objective third party is given

situation, can reasonably expect and infer that they are being observed.

(129) According to the Guidelines, it can reasonably be expected that examination and treatment rooms

you should expect surveillance, because the guests are in these rooms

intimate

they are visible in life situations, and camera surveillance seriously impairs the rights of those involved.

As a result of all this, the rights of the affected parties take precedence over the legitimate interests of the Company

enjoy, so camera surveillance in these rooms cannot be a proportionate measure.

(130) It follows from all of this, since the consent cited by the Company as a legal basis for data management

cannot be used in the case of data management related to camera monitoring of guests,

furthermore, since camera surveillance is not considered a proportionate measure, it is therefore justified

the Company could not prove the existence of its interest, therefore the Authority concludes that a

Company in the absence of a suitable legal basis - violated Article 6 of the General Data Protection Regulation

(1) paragraph.

V.5. Sound recording

(131) The Authority's position is that it causes more serious damage to the private sector if the cameras

sound is also recorded. According to the Authority's point of view, audio recording is also a

is considered to be data processing other than image recording, the legality of which and the associated right

the Company should have proven its interest separately during the procedure. The Company during the procedure

however, he did not present any circumstances that would support the audio recording

necessity.

(132) In relation to the scope of data management, the Authority found that the Company does not mention it anywhere

provides information that the cameras also record sound, which is a yes to data management

a significant circumstance that cannot be ignored, to which both employees,

all the guests can reasonably not even count, since there is nothing particularly clear

a reason that would support the need for audio recording, moreover, during treatment

recorded conversation and private information is not justified and completely unnecessary.

(133) Based on the above, the Authority concludes that the Company used a camera
data processing violates Article 6 (1) of the General Data Protection Regulation due to the audio recording
paragraph.

22

V.6. Fairness of data management

(134) The Company stated that it directed to employees' workstations, as well as the
monitors its employees with the cameras in the operators' rooms and in the training room for the purpose of
that the sales manager checks the employees' communication with the guests.
From this statement of the Company, it can be established that the electronic in the treatment rooms
the real and primary purpose of using a monitoring system is the sales activity
and with it the influence of employees' workplace behavior.

(135) Based on the statements made during the on-site inspection and the available recordings
furthermore, it was found that the guests in the recordings taken in the operators often
they are seen in incomplete clothing.

(136) Company
also in such premises
also uses camera surveillance, where a
employees spend their lunch time (training or training room).

(137) Based on the above, the Authority examined the extent to which the data management complied with the
the requirement of fair data management.

(138) The fairness of data management is closely related to the protection of human dignity, a
unfair data management behavior affects not only personal data
protection, but can also seriously violate the right to human dignity. As a result, the
the absolute limit of camera surveillance is the respect for human dignity, therefore
cameras cannot be operated by employees and their activities are permanent
nature observation. It can be considered illegal and unfair to do so electronically

the application of a monitoring system, which does not have an explicit, clearly defined

purpose, but only observes the work in general.

(139) Due to the principle of fair data management, cameras cannot be placed in particular

in the changing rooms, showers, and toilets, given that in these rooms

surveillance in particular violates the right to human dignity, in addition to the position of the Authority

also, it is not possible to use an electronic monitoring system in a room that

which has been designated for the purpose of taking employees' breaks between work, such as a

dining room for employees.

(140) The Constitutional Court in the 36/2005 (X.5) also pointed out electronic monitoring

and human dignity, when he said that "the camera, like the

the application of the technical means of property protection is suitable for the protection of property objects

yes, but inevitably to persons, human behaviors, customs, manifestations,

it can also be directed at the human body itself. Monitoring by electronic means is therefore

it is suitable for intruding into the private sphere, recording intimate (sensitive) life situations

in such a way that the person concerned does not even know about the recording or is not in a position to

to consider the admissibility of such recordings and their consequences. That's how it ended

observation beyond the violation of the right to privacy - in a broader and deeper sense - it is

it may affect the right to human dignity in general. It is the essential conceptual element of the private sphere

is that, despite the will of the person concerned, others cannot penetrate there, or even inside

to see. If the unwanted insight does happen, it is not only the

the right to privacy, but also other elements of entitlement within the scope of human dignity,

such as. freedom of self-determination or the right to physical and personal integrity may also be violated."

(141) Because of all these, the Authority found that the Company is the work for the employees

with its continuous monitoring aimed at influencing it, as well as for the purpose of eating

in the training room by observing the employees while they are relaxing,

also a

about guests in treatment rooms

continuous image and

violated Article 5 (1) a) of the General Data Protection Regulation with audio recordings

the principle of fair data management set out in point

made in intimate situations

23

V.6. The practice of accessing camera footage

(142) According to the Company's statement, the Company's managing director, head of HR, financial

the manager and the storekeeper can access it, but the need for their access rights is determined by the Authority

despite his call, he did not give a reason. During the on-site inspection, the Authority found that a

images of cameras in practice by clicking on the […] software shortcut and the

they are accessible to any employee by entering the same password as the username, such as

as the images of the cameras were also visible on the monitors in the open server room. In addition to the

there is also a computer in the warehouse from which the cameras can be accessed, so whoever enters the warehouse

enters, also has unlimited access to the recordings, and can view them without a specific purpose

and you can download it. Based on the Company's statement and the attached documents, the cameraman

does not have a data management policy, employees upon entry

they receive a one-time verbal information about the operation of the camera system.

(143) Integrity and confidentiality according to Article 5(1)(f) of the General Data Protection Regulation

arising from the principle of nature, as well as contained in Articles 24 and 25 of the General Data Protection Regulation

Based on the principle of built-in and default data protection, the data controller has the video camera

appropriate technical and organizational measures must be taken before starting monitoring

for data security. In this context, data and privacy belong to the data controller

must include guarantees for its protection not only in the technological design specifications,

but also into organizational practices.

(144) The data controller has a

for camera surveillance

provisions

when defining it, you must develop your procedure regarding who and where it is carried out

surveillance and who can access the video footage and for what purpose. The

in the area of data security, you must take measures to ensure that the system is only

authorized persons have access to it, and it must be ensured that the video recordings are stored

serving room should be protected from unsupervised access by third parties

opposite, and the monitors should be placed in such a way that only he is authorized to use them

people can see.

concerning

organizational

(145) Based on Article 32 (1) b) and (2) of the General Data Protection Regulation, the

in order to ensure the security of data management, the data controller must ensure it by controlling access

systems and services used to manage personal data must be kept confidential

nature, integrity, availability and resilience.

(146) What was experienced on site, as well as the attached documents and the Company's statements

based on this, the Authority determined that the Company did not guarantee the confidentiality of data management

nature, and the operation of the camera system did not protect personal data

measures, since he left the server cabinet open and for the images of the cameras,

as well as the stored recordings, without any applied purpose, he easily accessed the monitor

by typing a username written on a taped piece of paper.

(147) Based on all of this, the Company violated Article 5 (1) of the General Data Protection Regulation

point f), Articles 24 and 25 (2), and Article 32 (1)

point b) and paragraph (2).

V.7. Purposes and legal basis for processing the personal data of the Guests

(148) Employees of the Company's call center record the information published by the Company in the [...] database

persons applying based on advertising materials and offers published on the website, as well as a

the contact details of the persons filling out the consultation form. Calls from this database

are launched, and then the results of outgoing campaign calls, treatments and

the date of purchases, the reason for cancellations, refusals, in the case of concluding a contract a

also personal data provided during the conclusion of the contract.

24

(149) During the examination of the database, it was seen that the basic data of the guests included the Company

indicated when the given guest was included in the database, however, it was analyzed

data management could not be verified from any of the files or their columns

the provision of prior information necessary for its legality, nor the existence of the appropriate legal basis,

since no entry or information referring to this has been recorded in the database.

(150) As it can be seen from the above, the Company did not take any organizational measures which

and for the Authority

as a result of the data management

become known, the Authority found that the Company violated the GDPR

Article 5 (1) point a) of the Decree.

processes transparent,

V.7.1. Customer referral system

(151) In the examined database of the Company, there were 85 such records in the file called "Basic data".

can be found in which there was information indicating that the given person was recommended by someone else. This

further narrowing the scope of the subject to the persons with whom it could be identified

also the recommender, the Authority identified 44 records.

(152) According to the Company's statements, the recommendation system is subject to official control by the Company

on October 25, 2021.

(153) The customer recommendation system

the point is that the guests, as long as they are satisfied with one

service, for the purpose of first contact, they provide the contact details of their acquaintances

for the Company providing the service. During the customer recommendation system, it is typically recommended

the data is transferred without the person's knowledge or consent.

(154) In the referral system, the data of recommended persons are recorded in such a way that their

the data controller cannot properly verify its legal basis, namely the consent of the data subjects

it cannot be replaced by the bidder's statement. As a result, the data controller is not exempted

from data controller responsibility. In the referral system, also the identity of the recommending persons

is not recorded, or if it is, it is considered a new, independent data management,

to which the provisions of the general data protection regulation must also be applied.

(155) Since during the procedure, the Company did not take action as stipulated by the recommendation system

to verify the appropriate legal basis in connection with the data, the Company's recommendation practice is Article 6 of the

GDPR

(1) was in conflict. The initiation of official control of the recommendation system

due to the subsequent termination of the Authority, the Company's data management is a violation of law

it does not establish any further legal consequences.

V.7.2. The purpose and legal basis of managing the guest database

V.7.2.1. Legality of the processing of personal data processed in order to fulfill a contract

(156) According to the Company's current information on data management, the Company processes personal data

in order to fulfill the contract, then the name and phone number data are additional

it is also used for purposes such as organizing consultation appointments and acquiring business

and for information about personalized offers.

(157) Pursuant to the above, the information on the legal basis of data management is provided in this a

document, the Company states that the personal data provided during registration (name,

address, phone number, email address, information on purchases and services used,

correspondence) with the creation and maintenance of the contract between the guests and the Company and

it is handled in connection with its termination, in the absence of this, based on the consent of the persons concerned.

(158) Article 5(1)(a) of the General Data Protection Regulation stipulates that personal
processing data legally and fairly, as well as in a transparent manner for the data subject
must be done.

(159) Before starting data processing, the data controller must determine the planned data processing
appropriate legal basis for operations.

(160) Point b) of Article 6, paragraph (1) of the GDPR can be applied if the data management is with the data subject
is objectively necessary for the performance of the concluded contract, or is necessary for the data subject
take steps prior to entering into a contract at your request.

(161) If the data controller bases its data management on the fact that it is a contract with the data subject
necessary for its performance, its data processing is legal if the contract is applicable
is valid pursuant to contract law, and the data management provided to the data subject is valid
necessary to fulfill the contract. It follows that if the contract is complete
is terminated as a whole, as the processing of the data is no longer necessary for this contract
to fulfill, the data controller must comply with Article 17, paragraph (1) of the General Data Protection Regulation
point, you must delete them, unless the data management is in accordance with Article 17, paragraph 3, point b)
pursuant to the EU law applicable to the data controller, which prescribes the processing of personal data
obligation under Member State law, or legal claims under Article 17(3)(e).
are necessary for In this case, however, it is at the start of data management
stakeholders must be informed of how long the data will be kept for these purposes.

(162) With the "DEA migrated" value taken over from Beauty and More Kft., which previously operated the DeAura Center
regarding the transfer of the attached contract to the Authority regarding the data of the provided guests
according to the agreement, Beuty and More Kft. withdrawing from the contracts concluded with the guests
the Company has taken its place, and as a result, the Company has the rights and is bound by the contracts
also the obligations associated with its performance. According to the Authority's findings, Beauty and More Kft.-
for handling the data of guests received during the transfer of contracts concluded with GDPR Article 6 (1)

the legal basis according to paragraph b) can be applied.

(163) During the examination of the requested database, however, it was established that the Company is a guest

its database contains thousands of entries that cannot be linked to the Company

to guests with a contractual relationship, and the Company could not verify all of them

regarding your guest, that personal data managed on the basis of the contractual legal basis

can be linked to a specific valid contract, the Company has violated the general data protection

Article 6 (1) of the Decree.

V.7.2.2. Limitation of the processing of personal data processed in order to fulfill a contract

(164) Article 5(1)(b) of the General Data Protection Regulation establishes the principle of purpose-boundness

stipulates that the collection of personal data is only specified, clear and legal

purpose, and they cannot be handled in a manner incompatible with these purposes.

(165) Since it is not possible to track which guests are personal in the Company's database

your data is processed for contractual purposes, which are also for purposes other than this, the Company has violated the

The principle of purpose-bound data management contained in Article 5, paragraph (1) point b) of the GDPR.

V.7.2.3. Purpose and legal basis of data management for marketing purposes

(166) As the working group under Article 29 in 03/2013. in its opinion no

explained, the purpose of data collection must be defined clearly and concretely: sufficiently detailed

must be in order to be able to determine the nature of the data management, as well as

it must enable compliance with legislation to be assessed and is

data protection safeguards can be applied. For these reasons, a vague or general purpose,

such as "marketing purposes" - without further details - usually does not qualify

criteria of "uniqueness".

(167) In its prospectus, the Company mentions that "business acquisition" and "personalized

handles personal data for the purpose of providing information about offers", but this information a

based on the above, it does not meet the requirement of transparency, as it is too general and not

it is clear to those concerned what kind of data management it is and whether it is appropriate

for data management purposes.

(168) According to the Company's statement, the first contact with the Company was made by those concerned

initiated by filling out the application form. The online application form or the needs assessment

after filling out the form in person, the sale of various products and services of the Company

for the purpose of contacting those concerned and the result of the campaign, or the failure of the rejection

together with the reason, it is also recorded in its database. This activity of the Company is marketing

is considered an activity.

(169) Regarding the legal basis, the Company declared on April 5, 2022 that it treats

data for marketing purposes based on the consent given on the consultation form, this

after that, on September 28, 2022, he declared that he was managing based on the legitimate interest of the Company

guest data for marketing purposes, and then in a contradictory statement on October 14, 2022

I stated that it does not use guest data for such purposes, as it is for marketing purposes

data is only processed in relation to models and employees in social media

in the form of appearing video recordings. The legal basis for this data management is the recordings

the consent of the persons involved. According to the statement made by the Company on November 25, 2022

these contributions are recorded on a paper basis, which can be locked in a cabinet

are stored.

(170) After comparing the Company's statements, the Authority interpreted them as paper-based

under contributions, the Company includes, on the one hand, the signature of the consultation data sheet, and, on the other

hand, the models

and filled out by employees in connection with occasional appearances in commercials

means forms that the Company has been using since September 3, 2021.

(171) Since there is no section on direct marketing on the attached consultation sheets

would include consent to requests, concluded for the purpose of filming commercials

and contracts concluded for the purpose of directly soliciting guests are not considered

data management, the Authority did not accept the Company's statements that the consultation

for the processing of their personal data for marketing purposes for stakeholders who fill out forms

in writing

they contributed.

(172) The Authority examined the contact and application form on the Company's website

forms, on the basis of which he established that he is applying for the first treatment via the Internet

When sending the application, individuals can choose whether the Company requests information

discount offers, and whether they subscribe to the Company's newsletter service. THE

unsubscribing from the newsletter is done by clicking on the link at the bottom of the newsletters, a

the Company keeps a separate register of unsubscribers, which it sent to the Authority.

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

Regulation

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

considers the legal basis of legitimate interest as appropriate.

(174) In 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:

(175) Consent must be based on adequate information. The right information is the one on which

through the data processing of their personal data, and the

the right to informational self-determination can be asserted through information: that is data management

may be legal, the circumstances of which are fully known to the affected parties. The affected

13-14 of the general data protection regulation. article

details.

(176) The Authority to the Company regarding data management

examining your information

established that the Company neither in its information on data management nor in its consultation

on the data sheet, the data subjects do not provide any information about data processing for marketing purposes
for him, thereby the Company violated Article 13 (1)-(2) of the General Data Protection Regulation
paragraph.

(177) Another important component of the validity of consent is the will of the person concerned
its voluntariness, its freedom from external influence, which is realized when it is truly elective
option is available to the person concerned. If the consequences of the contribution are undermined
the individual's freedom of choice, the consent is not considered voluntary.

(178) A concrete, clear, unmistakable declaration or confirmation of the will of the person concerned
the requirement to declare it through an expressive act means, on the one hand, that a
consent must be active conduct, the omission of an active conduct [so
for example, not turning off a signal in a check box] cannot be considered
definite and unmistakable consent. On the other hand, clear, express consent
also purpose-assigned consent: given for a specific, specific data management purpose
can be considered as a contribution. As a general rule, the data is not used for other data management purposes
can be used.

(179) There are no statements or checkboxes on the consultation sheets that are marketing
would be aimed at allowing inquiries, so for those concerned who are not online
applied for treatment, but in person, the voluntariness of the consent cannot be proven
for marketing inquiries. There is a check box for people applying online
the possibility of filling it out, but at the same time, the Authority does not find any reference to it in the partner database
record which guest is the one who has consented to data processing for marketing purposes and which
partner is the one that doesn't. As a result, the Company's data processing for marketing purposes violated it
Article 6 (1) point a) of the GDPR.

(180) In 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 really exist

it must stand and actually exist.

(181) It is essential that the data controller must carry out an interest assessment to refer to this legal basis4.

Carrying out the interest assessment is 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 right of the data subjects to the protection of personal data, so

personal data that can be handled.

(182) The Company did not provide the Authority with a consideration of interests for marketing data management

regarding, as a result, the Authority did not accept that the Company's data management

is based on its legitimate interest, therefore the Company has violated Article 6 (1) of the GDPR.

V.8. Management of special categories of personal data

(183) The Company added to the appointments on the consultation sheets and in its database

it also records and stores the health data of those concerned in the comments section. The Company hereby

4 The Data Protection Working Group 6/2014 provides assistance in carrying out the interest assessment. No. is legal

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

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

referred to the fact that the processing of these special data is necessary in order to

the guests should not lose the pre-booked appointment.

(184) Health data, as by their nature particularly sensitive personal

processing of data only in specific cases, the general data protection regulation

is possible subject to stricter rules. In this context, the special data

processing is possible if the data subject has expressly consented to data processing, or

data management complies with Article 9 (2) of the General Data Protection Regulation.

(185) The consent will be "expressed" if the person concerned confirms in some way the

consent, and secondly, it also means that the person concerned is aware beyond any doubt

with the fact that it will apply to the special data of the data management and to their management

contributes. In addition, the consent requirement is met even if the service is concerned

about the request itself, which includes the processing of special data in connection with its use

informs the data controller, or the data subject specifically tailored to his own state of health,

you order a unique product from the data controller and during this process the fulfillment of the contract is impossible

without processing special data.

(186) The Company did not accept the Authority as proof of the express consent of the guests

statement according to which the data subjects are to handle the special data on the consultation data sheet

they agreed with their signature, as there is no part of the attached consultation data sheets where

guests could express the special personal data handling

their intention.

(187) In addition, since the Company did not substantiate in its answers that the individual

the management of health data is essential for the performance of the services it provides

would be necessary, or that postponing treatment appointments is not possible in any other way,

therefore, the Authority came to the conclusion that the Company did not handle it legally

affected personal health data and thereby violated general data protection

Article 6 and Article 9 (2) of the Decree.

VI. Legal consequences

(188) The Authority found ex officio that the Company violated it by monitoring the persons concerned

points a) and b) of Article 5 (1) of the GDPR as well as Article 6 (1) of the GDPR, therefore the GDPR

Based on points d) and g) of Article 58 (2), the Authority prohibits camera data management in
operators, as well as in the diagnostic and examination rooms, and also instructs the Company,
to cancel in a documented manner within 8 days of this decision becoming final
video recordings made in operators, as well as in diagnostic and examination rooms.

(189) The Authority found ex officio that the Company is responsible for the operation of the camera system
default settings that minimize data management, as well as personal data as possible
by failing to provide the means necessary for its highest level of protection
violated Article 5 (1), Articles 24 and 25 of the General Data Protection Regulation, and
Article 32, paragraph (1), point b) and paragraph (2). For this reason, the Authority classified the Company in accordance with
Article 58 of the GDPR.
is convicted according to Article (2) point b) and pursuant to Article 58 point d) of the GDPR
instructs you to take the appropriate technical and organizational measures in order to
that its data management operations are in accordance with legal provisions.

(190) The Authority established ex officio that by recording the guests' health data a
Company violated Article 6 and Article 9 (2) of the GDPR, therefore the Authority
Based on points d) and g) of Article 58 (2), it prohibits in connection with reservations a
management of guests' health data and instructs the Company to end it
health data in the comments to appointments in your database
recording, and also instructs you to delete from the comments attached to the appointments
personal health data of data subjects.

(191) The Authority found ex officio that since the Company treated the guests without a legal basis
your data for marketing purposes, and therefore violated Article 6 of the GDPR in relation to this data management
(1) paragraph. For all these reasons, based on point d) of Article 58 (2) of the GDPR, the Authority
instructs the Company to stop illegal data processing and data processing
bring the operation into line with the legal provisions by verifying the guests

the legal basis for processing your data for marketing purposes.

(192) Based on point d) of Article 58 (2) of the GDPR, the Authority ex officio instructs the Company to

to delete personal data processed through customer referrals from its database.

(193) The Authority ex officio examined whether it was justified due to the established violations of the

Imposition of a data protection fine against the company.

(194) In this context, the Authority is required by Article 83 (2) of the General Data Protection Regulation and Infotv. 75/A.

considered all the circumstances of the case based on §. Given the circumstances of the case, it is

to the nature of data management, the Authority found that the violation revealed during this procedure

in the case of the warning is neither a proportionate nor a deterrent sanction, therefore a fine

it is necessary to impose it on the basis of Article 58 (2) point (i) of the GDPR.

(195) Violations committed by the Company are Article 83 (5) of the General Data Protection Regulation

According to points a) b) g) and k), belonging to the higher fine category is more serious

are considered a violation of law. Based on the nature of the violations, the upper limit of the fine that can be imposed is

20,000,000 EUR based on Article 83 (5) points a) and b) of the General Data Protection Regulation,

or a maximum of 4% of the total world market turnover of the previous financial year, provided that the two

the higher amount must be imposed.

(196) The Company's net sales in 2021 were HUF 216,190,000. Given that the Company

an amount representing no more than 4% of the total annual world market turnover of the previous financial year 8,647,600

HUF, which is an amount lower than EUR 20,000,000, the maximum possible fine

20,000,000 EUR.

(197) When determining the amount of the fine, the Authority considers the following circumstances aggravating

considered as a circumstance:

- In terms of their nature, the violations committed by the Company are considered to be more serious violations,

whereas the Company, regarding the legality of data processing (legal basis) and rights of stakeholders

violated relevant provisions [GDPR Article 83 (2) point a)];

- The violations committed by the Company continued for years [GDPR Article 83 (2)

paragraph point a)],

- The Company has committed several serious violations of the law in its data management activities

is blatantly illegal, especially given that the Company's data management with the camera

also violated the principle of fair data management. [GDPR Article 83(2)(a)];

- In 2021, the Company carried out cosmetic procedures on a total of 7,789 guests 11,935 times

treatments, and 2,218,913 related to 357,157 persons in the database files

registration, and there are also 2,218,913 communication records, hence the number of those affected

considered high [GDPR Article 83(2)(a)];

- The established violations were caused by the Company's grossly negligent behavior. [GDPR

Article 83(2)(b)];

- The violations also affect the special category of personal data, the handling of which is significant

carries a risk. In addition, according to the Authority's point of view, for those concerned

data management through the camera system results in a more harmful situation if a

in recordings, they are not in general street clothes, but in more incomplete clothes, therefore a

Illegal handling of personal data in recordings recorded in operators is greater

has material weight. [GDPR Article 83(2)(g)];

30

(198) During the imposition of the fine, the Authority assessed the following circumstances as mitigating circumstances:

- The Company has not previously committed a data protection matter under the scope of the GDPR

breach of law [GDPR Article 83(2)(e)];

- the Authority exceeded Infotv during the procedure. 60/A. Administrative according to paragraph (1) of §

deadline [GDPR Article 83 (2) k)].

- According to the Company's statement, it has discontinued the use of the customer recommendation system [GDPR

Article 83(2)(f)]

(199) When determining the amount of the data protection fine, the amount of the fine was not aggravated and

it was not mitigated by the fact that the Company did not recognize the violation and because of this

did not take any mitigation measures [GDPR Article 83(2)(c)].

(200) The Company ordered a temporary measure in order to mitigate the impact on the rights of those concerned he confirmed the implementation of the measure only upon repeated calls from the Authority, and at the same time the Authority did not take this circumstance into account when determining the amount of the data protection fine in view of the fact that during the procedure the Company was required in the general data protection regulation due to violation of his obligation to cooperate, he was fined [GDPR Article 83 (2) point (f)].

(201) The Authority did not consider the general data protection regulation relevant when imposing the fine circumstances according to Article 83 (2) d), h), i) and j), as they are related to the specific case are not interpretable.

(202) The amount of the fine was determined by the Authority acting within its statutory discretion and, during which it was taken into account for the simplified annual report of the Company for 2021 also its balance sheet contained in the attached supplementary annex. According to this, in 2021 the Company will have 216,190,000 HUF with sales revenue, HUF 127,940,000 in current assets, and HUF 51,510,000 in tangible assets provided, including from the "lease" contracts entered into by the Company for cosmetic treatments outstanding claims as well.

(203) Since the established violations involve a wide range of both the Company's employees and its guests are affected, and due to the monitoring of the Company's guests, the Authority may inform Infotv. § 61. (2) a) and Based on point c) of this decision, he considers it justified to publish the Company's data disclosure.

(204) On the basis of the above, the Authority made a decision in accordance with the statutory part.

VII. Other questions

(205) Based on the facts revealed during the procedure, the Authority found that unfair market behavior and LVII of 1996 on the prohibition of competition restrictions. violation of the provisions of the law

in order to examine this decision and the documents generated during the procedure

for the purpose of its initiation, it sends it to the Economic and Competition Office.

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

covers the entire territory of the country.

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

Based on § 82, paragraph (1), it becomes final upon its publication.

(208) The Art. § 112 and § 116, paragraph (1) and § 114, paragraph (1) with the decision

on the other hand, there is room for legal redress through a public administrative lawsuit.

(209) The rules of the administrative procedure are laid down 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. Section 13,

paragraph (3).

Based on point a) subpoint aa), the Metropolitan Court is exclusively competent. The Kp. Section 27 (1)

legal representation is mandatory in a lawsuit falling under the jurisdiction of the court based on paragraph b).

The Kp. According to paragraph (6) of § 39, the submission of a claim is an administrative act

does not have the effect of postponing its entry into force.

(210) The Kp. Paragraph (1) of § 29 and, in view of this, Pp. According to § 604, the electronic one is applicable

CCXXII of 2015 on the general rules of administration and trust services. law (a

hereinafter: E-administration act) according to § 9, paragraph (1), point b) of the customer's legal representative

obliged to maintain electronic contact.

(211) The time and place of filing the statement of claim is specified in Kp. It is defined by § 39, paragraph (1). THE

information on the possibility of a request to hold a hearing in Kp. Paragraphs (1)-(2) of § 77

is based on. 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.

Dated: Budapest, according to electronic signature

Dr. Attila Péterfalvi

president

c. professor