Case number: NAIH / 2019/55/5.

Subject: Organized by Sziget Zrt

at events with admission

examination of related data processing

H AT PRICE O Z AT

The National Data Protection and Freedom of Information Authority (hereinafter: the Authority) is the Island

Cultural Manager's Office Private Limited Company (registered office: 1033 Budapest,

Shipyard island hrsz. 23796/58, company registration number: 01-10-049598; hereinafter referred to as "the Debtor"), and

at events organized by its predecessor in the period from 2016 to 24 May 2018,

access - related data management on the right to information self - determination; and

CXII of 2011 on freedom of information (hereinafter: the Information Act) and the 2018.

at events organized after May 25, related to admission

processing of personal data by natural persons

the free movement of such data and repealing Directive 95/46 / EC

Regulation (EU) No 2016/679 of the European Parliament and of the Council of

initiated ex officio to investigate compliance with the Regulation)

makes the following decisions:.

1. The Authority shall determine the costs incurred by the Debtor from 1 June 2016 to 24 May 2018.

implemented during the admission practice used at events organized during the period

unlawfulness of data processing in respect of the data subject by the Debtor during the period under review

data management

(a) on an incorrect legal basis,

b) did not comply with the purpose limitation principle,

(c) the persons concerned have not been given adequate prior information.

2. The Authority shall determine the organization organized by the Debtor after 25 May 2018

the illegality of the data processing carried out during the entry practice applied at the events

in respect of the Debtor during the period under review

(a) on an inappropriate legal basis,

(b) breach of the principles of purpose and data protection

processed the personal data of the data subjects.

3. The Authority shall order the Debtor to comply with the data management practices applied during entry

bring it into line with the rules of the General Data Protection Regulation.

2

4. The Authority shall notify the Debtor at events organized by it after 25 May 2018

30 days after the entry into force of this Decision due to unlawful data processing

within

HUF 30,000,000, ie thirty million forints

data protection fine

obliges to pay.

5. The Authority shall at the same time order the disclosure of this Decision with identifying information

on your website.

The measures taken by the Debtor shall govern the initiation of judicial review

shall inform the Authority within 30 days of the expiry of the time limit for bringing proceedings.

The fine is paid by the Authority's forint settlement account for the collection of centralized revenues

(10032000010404 25-00000000 Centralized collection account IBAN: HU83 1003 2000 0104 0425 0000 0000)

to be paid for. When transferring the amount, NAIH / 2019/55/5. JUDGE. number should be referred to.

If the Debtor fails to meet the obligation to pay the fine within the time limit, a late payment allowance

is obliged to pay. The rate of the late payment interest is the statutory interest, which is the calendar affected by the delay

equal to the central bank base rate valid on the first day of the first half of the year. Fines and penalties for late payment

in the event of non-payment, the Authority shall order enforcement of the decision, a fine and a penalty payment

recovery of taxes.

There is no administrative remedy against this decision, but it has been available since its notification

Within 30 days, an action brought before the Metropolitan Court may be challenged in an administrative lawsuit. THE

the application shall be submitted to the Authority, by electronic means, which shall forward it together with the file

to the court. The request for a hearing must be indicated in the application. The whole personal

for those who do not benefit from an exemption, the fee for the court review procedure is HUF 30,000;

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

EXPLANATORY STATEMENT

I. Procedure and clarification of the facts

I.1. Background, investigation by the Authority

The Authority was previously notified under NAIH / 2016/4278 / V. and NAIH / 2017/3208 / V. investigation procedure

The legal predecessor of the Debtor, Sziget Cultural Management Office Ltd. (hereinafter: Sziget Ltd.,

Ltd.).

I.1.1. Legal basis for data management

The Authority received complaints in connection with the VOLT Festival in 2016, the applicants in this

The practice of Sziget Kft. At admission, during which the

the identity card of the guests and that they are not properly informed

the conditions of data processing, such as the purpose and duration of personal data

copies of the ID cards for which they are used.

Based on the data management information of Sziget Kft. Valid during the examined period, the Kft

marked data management during the login process as a separate data management, which

read, recorded and recorded the following data on the data subject in the identity document

stored: citizenship, name, type of document, number, expiration date, date of birth, no. At the same time

a video and audio recording of the data subject was made, which was also “recorded, stored and managed” by the Kft.

Section 4 of the data protection information available in June 2016 - during the VOLT Festival - contained

"Identification during the entry process". Based on this, “by the data controller

registration at the venue of the events to be held (ie an armband

during the assignment to a natural person identified during the entry process)

The data controller requests proof of identity with a photo ID. Of this

the Data Controller reads the data recorded in the personal identification document about the data subject,

records, stores and manages, as well as video and audio recordings of the data subject, which are also recorded and stored

and treats ".

Sziget Kft. Reserves the right not to provide the above to the person concerned

consent, he could invalidate the armband and refuse entry to the event.

In August 2016, Sziget Kft. Modified its data management practices for the duration of the SZIGET Festival,

however, in the prospectus, it maintained the previous status 1.4 as regards the legal basis for data processing.

the consent, and therefore extended it to the entry process:

The legal basis for the processing of data by the data controller is the informed consent of the data subjects, which is provided

by the customers

during registration by accepting the registration conditions, while during the entry process

identification by participation in it ".

The Authority shall issue NAIH / 2017/3208 / V dated 15 June 2017. ('the first letter')

notice) informed Sziget Kft. that in the absence of volunteering, the data subject did not consent

considers it an appropriate legal basis for the processing of access data.

In its letter of 19 July 2017, in response to the letter of formal notice, Sziget Kft.

those involved have a real choice, as the admission practice only needs to

submit to a ticket to the event. In their view, since the ticket

purchase is not mandatory for those concerned, so they are in a real choice, so

continued to rely on stakeholder consent as the legal basis for data management in 2017

during organized festivals.

I.1.2. Purpose of data management

Among the purposes of the data management associated with the access control system, the Ltd. stated that the design of the

system

started after the terrorist attacks in Paris in November 2015, when it was decided that the

Sziget Kft. Will apply an entry system in which the armband is received upon receipt

its holder will be named. In his opinion, the mass events of Sziget Kft. - like everything else

are exposed to a serious terrorist threat. They referred to it

also that "foreign and foreign service agencies in different countries have warned in turn that - others

In addition, events similar to those of Sziget Kft. may become targets of attacks in the future ".

He also reported contact with “national security services” and other authorities

kept up to help with their work. The establishment of an entry system also served to provide

a “specialist service” acquires relevant information for an action in preparation, so

Sziget Kft. should be able to filter out the persons designated by the authorities. During system operation

because it is possible to know that a given person (based on personal identification data or a photo)

has entered the event, or this person may be prevented from attending the event.

In their view, taking these precautions cannot be considered disproportionate to the threat, as

necessary means to endanger the safety, physical integrity or life of visitors

prevent.

In its statement, it also informed the Authority that it was described in section 4 of the Privacy Notice

unlike the VOLT Festival and Balaton Sound, the legal basis for data management is Infotv. Section 6 (5)

was the personal security of the visitors attending the mass event

in order to preserve it. The Data Management Information Sheet, as mentioned earlier, has been amended for the duration of

the 2016 Sziget Festival, the legal basis has become the consent of the stakeholders.

In its view, the protection of the personal safety of participants in a mass event is proportionate to

by restricting the right of visitors to the protection of personal data as set out above

also that the data recorded at the time of entry was deleted within 72 hours after the event.

In his opinion, there is no other way to quickly enter such a large number of people at a festival

in addition to the objectives set out above. Sziget Kft. Uses the data in its own internal database

stored on the servers, at the venue of each event and at the headquarters of the Ltd., the data was stored in 3MAT9000 passportscanner, the photo information was retrieved when the visitor entered the festival area, or the document image in the case of an old type of identity card.

The data was stored and processed for 72 hours after the official closing of the event, after which they were have been deleted definitively, unless an act has occurred which justified the data further storage (in this case the data have been kept for a maximum of 1 year or, if required by an authority, the have been retained for a period to be determined by it).

He also emphasized that "Sziget Kft. Does not transfer the data to third parties and databases, circling lists, as you cannot and do not want to take over the emphasizes the possibility of this in its external communication the deterrent effect of the system ".

Regarding the Authority's question on access rights, Sziget Kft. admissions staff will see what kind of photo will be recorded for that wristband, however these employees cannot see the database, they cannot search it.

It did not show the document pictures to the admissions staff at the time of entry, only the visitor's photo. The document image was used by the Ltd. at the time of entry only if they were told if the card was not suitable only for extracting the photograph (old type cards case). In addition to the identification at the time of handover and entry with the wristband, or however, with the exception of any inquiries, they claim to have taken photographs and documentary images not used by Sziget Kft. Only Sziget Kft. Has the highest level of access to the database itself employees (approximately 20), but only for the purpose of be able to comply with official requests.

Following the above statements of Sziget Kft., The Authority contacted the police, the Constitutional Court Office and the Counter-Terrorism Center (hereinafter: TEK).

1 Infotv. Pursuant to Section 6 (5), “if the personal data were collected with the consent of the data subject, the data controller shall

in the absence of a provision

(a) to fulfill a legal obligation to which it is subject; or

(b) for the purpose of enforcing a legitimate interest of the controller or of a third party, where the exercise of that interest is a

right to the protection of personal data

proportionate to the restriction

without further consent and after the withdrawal of the data subject's consent. "

5

The National Police Headquarters reported to the local capitals and Sziget Kft.

cooperation and whether there has been any other involvement in the jurisdiction

during a festival held in their territory. They also provided information that no data was requested for the Island

Ltd., however, several inquiries were sent for their investigation

to Sziget Kft. However, it was explained that the significant was considered professionally supportable

measures taken by the organizers of events attracting crowds which increase the

the security of the participants as far as the data subjects are concerned, in particular their personal data

they receive adequate information about the purpose and duration of the processing of their data and the possibilities of their

use

and knowing this, they decided to buy tickets.

The Office for the Protection of the Constitution reported that it did not request a national security risk from Sziget Kft.

with reference to the occurrence of personal information, however, supports similar events

in support of national security (counter-terrorism) activities

the development of uniform data management practices.

TEK informed the Authority about the consultation with Sziget Kft.

on the transfer of data and its legal basis and their handling. According to their statement

the data required were the birth name, date of birth, and date of entry of the persons admitted.

TEK also reported that it only requested the data of the visitors of the Sziget Festival from Sziget Kft.,

they did not request data from the data management of the additional festivals they organized.

In their view, the terrorist threat of large-scale events is higher than others

events, which requires more caution on both the part of the organizers and more

even for TEK, their statutory tasks against terrorism are a task

during its implementation. However, it was stressed that the personal data access control system

and its operation must comply with the legal provisions on data processing.

In its first letter of formal notice, the Authority stated that, in its view, the practice did not

is suitable for achieving the data management goals indicated by the Ltd., nor is it essential for that purpose

called on the Ltd. to transform its entry system and practice to meet the

applicable legal requirements, with particular emphasis on justifying data processing

suitability and indispensability.

In its reply dated 19 July 2017, Sziget Kft. Reported that it was employed by them

access control system - during which the wristband is scanned during personalization

identity card of visitors - considered appropriate and essential for

to achieve data management purposes. In their view, the prevention of possible terrorist acts

an end in itself where the measures they introduce cannot be considered

disproportionate. On-site identification of entrants - even if this is not done in advance

Considered effective, which in their view can significantly reduce the risk of

terrorist threat. The perpetrators may fear that the identification and

during video recording, they get stuck in the filter and are highlighted, even for the festival.

before entry. In their view, this is no other reasonable solution under festival conditions

unable to provide.

I.1.3. Purpose of data management

The investigation of the Authority also covered whether the Ltd. provided adequate prior information to the investigated entity

data management for festival-goers during the period.

According to the data protection regulations in force at that time, Sziget Kft. - as a data controller - is the festival

The following four data processing operations were identified in connection with the

1)

2)

3)

4)

collected during ticket purchase;

related to sending newsletters

completed during admission; and

within the event, the data management related to its organization.

The data management related to access is regulated primarily by the visitors

protection of personal security and, secondly, the prevention of misuse of access

justified.

Sziget Kft. Indicated the consent of the data subject with respect to all data processing indicated above.

as a legal basis for the processing of personal data, for example during the purchase of tickets

at the beginning of the entry process, while at the time of identification during the entry process

By giving his consent, the data subject shall give his consent.

The wristband that allows access is defined as natural during the entry process

when assigning a data to a person, the data controller shall be photographed

requested proof of identity. Fulfilling this - according to the regulations -

was a prerequisite for attending the event, therefore, when entering the festival

According to his approach, the data subject gave his or her express, prior and voluntary consent in person

for the processing of your data by the data controller.

The data controller also informed the data subjects that it was a law or a court or official

in the case of an obligation to the person (s) specified therein within the scope specified therein

may transfer, make available or otherwise handle the personal data of data subjects

you can connect.

According to the prospectus, the personal data processed about the data subject is official of Sziget Kft

72 hours after closing, where they were recorded, unless

there is a well-founded suspicion of abuse, or the life and physical integrity of the participants at the event

or an act which is prejudicial to, threatening or endangering his health has taken place. In this case

the data for more than 72 hours, but not more than one year, or in the case of a different obligation of the authority

for the period specified therein.

In its first request, the Authority stated that the information concerning the data processing under investigation

did not comply with Infotv. Section 20 (2) in force during the investigation period, and

he therefore called on him to bring his information into line with the provisions of the law and - the others

data management practices.

After Sziget Kft. Did not comply with the provisions of the first notice, the Authority once again

Sziget Kft. Also dated its reply letter dated 19 July 2017 - dated 20 December 2017

In his letter, he repeatedly called on Sziget Kft. to review and shape its data management practices

in accordance with the legal provisions in force and to modify its access control system

in such a way as to comply with the provisions in force, in particular with regard to the appropriate legal basis for data

processing

legal requirements.

The Debtor received the notice dated December 20, 2017 on January 4, 2018, January 2018

On the 11th day, he submitted a request for an extension of the 60-day deadline, which is included in the notice

has not been complied with until the commencement of the official proceedings in the above case.

I.2. Official procedure

7

Following the above history, the Authority received a notification on 16 July 2018 in which a

The applicant submitted that the condition for admission to the VOLT festival in June 2018 was

copying the identity card of persons wishing to enter.

In view of the above, on 8 October 2018, the Authority initiated ex officio official proceedings against the Debtor.

by

a) at events organized in the period from 2016 to 24 May 2018,

data processing related to access (essentially examined in the previous investigation procedure

data processing) to Infotv., yel, and

(b) admission to events organized after 25 May 2018

compliance with the general data protection regulation

to examine.

On 31 December 2017, Sziget Kft. Was transformed into a private limited company, so a

Authority initiated the official proceedings of the Sziget Cultural Manager's Office Private Limited Company

launched against.

I.2.1. Framework for data management related to access

In a letter dated 25 October 2018 from the Debtor in response to the Authority's request for information

stated that it had complied with the request in the previous investigation procedure,

reviewed and restructured its data management practices, but for "administrative reasons"

failed to inform the Authority.

The Debtor stated that he would use the same practice at the major festivals he organized, so that the

Sziget Festival, the VOLT Festival and the Balaton Sound Festival (hereinafter together:

festival), so that his declarations for all three festivals

to be understood.

The Debtor stated that the condition for entering the festival was the personalization of the tickets, which

that in the case of a pre-purchased ticket from the Obligor, at the exchange point on the spot, at the

in the case of ticket purchases, read from the identity document at the on-site ticket office - but the document

without copying - records the visitor's first and last name, date of birth, origin

country, nationality and sex and shall record the photograph on the document or, if

It is not possible to capture a photo on a document for technical reasons, it will take a photo on the spot

about the data subject.

When replacing the wristband, the Debtor assigns the visitor's personal data to the wristband, and
the visitor's rights (on which days he is entitled to enter the festival area, which campsite
entitled to enter) on the so-called Using an RFID chip, which makes the wristband electronic
ID.
At the access gates, the RFID chip is then read at each entry,
the Debtor thereby checks at each entry whether the visitor is entitled to enter the festival
(is your ticket valid for that day) or that the
whether the person assigned to the armband and thus authorized to enter intends to enter.
At the access gates for display on the monitor in front of the access staff for this control
the image, name, gender and date of birth of the person wishing to enter (ie check-in details)
narrowed scope).
The Debtor stated that he would not handle copies of the document, extracted from the document or manually
and for the storage of recorded data in the operation of Netpositive Kft., which is owned by the Debtor

on the server located at the venue of the event, as well as on the device located in the Telekom Server Hotel at 1822 Victor
Hugo utca, 1132 Budapest.
The Debtor submitted that the data processed by him should be submitted no later than 72 hours after the closing of the
festival.
permanently deletes this statement by the Debtor regarding the erasure of data at the 2018 festivals.
confirmed by sending minutes.
I.2.2. Balance of interest test performed by the Debtor
The Debtor stated that the processing of data during entry is a general data protection regulation
Article 6 (1) (f), the prevention of abuse and the personal identification of visitors
in order to ensure the security of both the Debtor and the data subject
and the legitimate interest of visitors. In order to prove the legitimate interest, the Debtor sent the
On March 20, 2018, he conducted an interest balance test.

The balancing test identifies two areas of interest: the Debtor 's economic interest in

the tickets it sells should not be misused and visitors should be for life and personal

security interest and the interest in the organization of the Compulsory Event, which

it is an essential condition for providing a safe environment for visitors.

the)

According to the test, prior to the introduction of this practice, the Mandatory was merely armbands

(where and when the wristband was issued), so

it happened that ticket sellers bought the ticket at the box office and then at a higher price

resold. As the ticket was not personal, a "ticket giver"

purchased more tickets, triggered the armbands, then replaced the armbands already triggered

resold at a higher price.

According to the Debtor's statement, it has also happened that someone has stolen a festival ticket from the box office,

then he entered the festival with it, and the Debtor could not identify the stolen tickets.

It was also common for several people to enter the festival one after the other with an armband

to the venue because the guests 'unused armbands were purchased by ticket gunners and then

resold.

b)

The interest balance test briefly summarizes the 2015-17. years

terrorist attacks on the basis of which the Debtor has established that the terrorist threat is real

phenomenon, which is a potential target for music festivals that attract large numbers of visitors, so

the Balaton Sound, VOLT festival and the Sziget festival organized by the Debtor.

Based on all this, the test identified the right of festival-goers to life and personal safety,

which, according to the Debtor, is a fundamental human right.

According to the test, the physical screening of visitors at check-in is not an end in itself

as the festivals are held in an area that anyone can during the year

are open to the public, so that, where appropriate, the “living and

personal security measures ”and as the areas are not available to the Debtor throughout the year

under their control, so that they cannot be fully scrutinized.

The test includes that the data subject of the procedure - with physical security measures

together to identify ‘potential perpetrators’.

9

In this regard, the test details that, if appropriate, an act of terrorism may follow

to prevent or deter the Debtor from paying attention to the designation by the authorities

whether persons have entered or attempted to enter the festival grounds.

The test also states that the practice used is not merely an act of terrorism, but “the

screening potential perpetrators of violent or drug-related crime

can serve ”.

According to the balancing test, this practice is not merely special but general prevention

it can also be a deterrent to anyone planning to do so.

to commit.

According to the test, it is also necessary to assign the specified data to the wristband because it a

experience that festival-goers do not keep personal identities in the days following entry

their document.

In the interest balance test, the Debtor examined the rights and interests of the data subjects

restrictions during the entry system. According to the Debtor in general

it can be said that the data subjects do not want to store or process their personal data.

The balance of interest test includes that during the festival and 72 hours after the festival closes

the personal data of the visitors are in the possession of the Debtor in the manner mentioned above, a

will be permanently deleted or anonymised 72 hours after the end of the event.

Personal data will not be used beyond access control, no

do not link them to other data of the Debtor.

According to the test, the method used in practice has long been used on physical lines of defense

it also provides visitors with psychological protection beyond that, as data can be stored for a short period of time

in the event of suspicion of terrorist offenses or other criminal offenses

their prevention through the information obtained from the database.

According to the test, the admission practice is also favorable because by applying this practice a

access is faster, there are no such long lines at the access gates, the smaller ones

and crowd, according to the Debtor, is a less attractive target for potential perpetrators.

According to the Debtor, due to all these arguments, the interest of the personal security of the visitors and the

Your interest in avoiding mandatory abuse is an interest that takes precedence over your visitors

against the right to the protection of personal data.

The Authority had further questions regarding the balancing test,

in a further order sent to the Authority in order to clarify the facts.

- by letter dated 18 January 2019.

The Debtor stated at the Authority's request that it did not use a special algorithm or did not fit

add to any records that would screen those who pose a threat. He performed

and to decide, on the basis of an official signal, which person presents a potential hazard, and

considers it necessary to apply an access control system in order to screen out persons designated by the competent

authorities. The Debtor emphasized in his response that he was not using it

database to identify potential individuals.

The Debtor stated that after the introduction of the system, the number of offenses in question

steadily declining. This statement of the Debtor is dated 17 August 2017, attached,

with the professional statement issued by In-Kal Security Events Kft. (hereinafter: In-Kal), and a

https://nepszava.hu/1137942_iden-a-magyarok-hoztak-a-sziget-nyereseget,

https://hvg.hu/itthon/20180815_Joval_kevesebb_buncselekmeny_tortent_a_Szigeten_mint_tavaly,

with press articles on the websites

https://www.vg.hu/kozelet/kozeleti-hirek/visszaesett-a-buncselekmenyek-szama-a-szigeten1049502/ / latest-hires /

organizational-news / island-iden-less-buneset-a-festival-side

confirmed by an official statement from the

All press articles on the announcements of the Budapest Police Headquarters (hereinafter: BRFK)

reports: Népszava article writes about the 2017 Sziget Festival, according to which the 2017 festival increased by 16%

fewer crimes were committed than at the 2016 festival; on the website of HVG and World Economy

articles in connection with the 2018 festival report that by 51% this year

fewer crimes were committed than at the 2017 event.

All press articles, as well as the BRKF statement, praise the work of the police, according to which the

security has also worked hard at external venues and inside the festival

on the entry practice used by the Debtor,

none of the press articles writes about its suitability and impact on the development of criminal offenses.

In the professional statement given by In-Kal, Dr. Kázmér Lovas explains that the so-called “Checkin” system has improved the

Debtor’s events with unexpected efficiency and effectiveness

the general security of the system, as it considered that the presence of the system had led to an unwanted fall

The appearance of “guests,” the presence of “dealers” has demonstrably declined, the smaller one

and crimes have almost completely disappeared.

I.2.3. The scope and necessity of the data processed by the Debtor in connection with the entry

The Debtor shall be informed of the scope of the data processed (surname and first name, date of birth, country of origin,

nationality, gender and image) that it was narrower than in previous practice

data type, as it no longer records the type of document, the authority issuing the document, the expiry date of the document

and the document identification number.

The Debtor stated that it was necessary to handle all the data named by him

to attempt or commit an abuse or to threaten security

the person causing danger can be clearly and unequivocally identified.

the)

Debtor - in another order sent to the Authority to clarify the facts

by letter of 18 January 2019, he stated that

to establish the right of entry of a person seeking entry is merely

your portrait will appear on the monitor in front of the access staff.

The Debtor justified this statement on the grounds that it was common for the person to obtain a passport

the extracted image does not exactly match the current portrait of the person, and it also happens that the weekly

the person with the ticket is different from the picture taken of him on the first day of the festival

will have a look.

According to the Debtor, in addition to the image, the name, date of birth and gender of the visitor

it is necessary to display it on the access monitor because so the access staff is in control

the person wishing to enter can be convinced without any doubt as to the conditions of the questions

identity.

b)

The Debtor stated that, given the high number of foreign visitors, the number of visitors

the country of origin, ie the issuing authority, is

to establish that a possible terrorist offense or other criminal offense

in which case the foreign authority of the country shall be notified.

c)

The Debtor stated that the nationality or citizenship was recorded for that purpose

necessary, where appropriate, in the event of a terrorist offense or other act

as a result, the visitor would lose consciousness and subsequently recover or be in a state of shock

the language in which the data subject can be communicated.

The Debtor - in another order sent to the Authority in order to clarify the facts

In his letter of 18 January 2019, he emphasized that

in the general case, it is not read - so it does not appear on the monitor when you log in - but

only in exceptional and justified cases will this information be made available.

In response to a question from the Authority, the Debtor also stated in this letter that during the 2018 festival season, without

claiming to be exhaustive, English, German, French, Dutch, Spanish, Slovak, Czech, Russian,

volunteers able to interpret in Ukrainian, Italian, Turkish and Hebrew were available.

II. Applicable law

In the course of the Authority's proceedings, the CXXX of 2010 on legislation. Section 15 (1) of the Act (hereinafter: Jat.)

Subject to points (a) and (2) (a), the lawfulness of the processing shall be the subject of the proceedings

the legal provisions in force during the period of implementation of the data processing operations

and, since it is inseparable from the underlying substantive legal obligation,

applied the same rules to the legal consequences established. The official

However, with regard to the procedural rules governing the procedure, Jat. Section 15 (1) (b)

subject to the legal provisions in force at the time the proceedings are initiated.

II.1. For data management from 2016 to 24 May 2018

Infotv. Pursuant to Section 4 (1), personal data is used for a specific purpose only

and can be managed to meet an obligation. It is necessary at all stages of data management

comply with the purpose of the processing, the fair collection and processing of the data, and

must be legal.

Infotv. Pursuant to Section 5 (1), personal data may be processed if

(a) the data subject consents thereto, or

(b) by law or, as authorized by law, within the limits specified therein

by a decree of a local government for a purpose based on the public interest (hereinafter: mandatory data processing).

Infotv. Pursuant to Section 6 (1), personal data may be processed even if the data subject

obtaining your consent would be impossible or disproportionate and personal data

his treatment

(a) necessary to fulfill a legal obligation to which the controller is subject, or

(b) necessary for the legitimate interest of the controller or of a third party, and

enforcement is proportionate to the restriction of the right to the protection of personal data.

Infotv. Pursuant to Section 4 (2), only personal data that is data processing may be processed
essential for the attainment of that objective and capable of attaining that objective. Personal information is for purposes only
to the extent and for the time necessary to achieve its
Infotv. Pursuant to Section 20 (1), the data subject must be informed before the start of data processing that
data processing is based on consent or mandatory.
12
Infotv. Pursuant to Section 20 (2), the data subject shall be clearly and
shall be informed in detail of all facts relating to the processing of your data, in particular:
the purpose and legal basis of the data processing, the person entitled to the data processing and data processing,
on the duration of the data processing, if the personal data of the data subject are processed by the data controller in
accordance with Section 6 (5)
and who may have access to the data. The information should be out
extend to the data subject's rights and remedies in relation to the processing.
In the course of the implementation of the first phase of data management of Infotv, before the entry into force of the GDPR,
Pursuant to Section 61 (1) (a) and (g), in its decision in the data protection authority proceedings, the
Authority may, inter alia, establish the unlawful processing of personal data or
may impose a fine of one hundred thousand to twenty million forints
can spread.
Act XXXIV of 2004 on small and medium-sized enterprises and support for their development Act (a
hereinafter: Kkvtv.), an enterprise whose
(a) has a total number of employees of less than 250, and
b) annual net sales amounting to a maximum of HUF 50 million or balance sheet total
an amount of up to EUR 43 million.
The SME 12 / A. § (1), the bodies carrying out official inspections shall
against medium-sized enterprises in the event of an infringement in the first case - the tax and
customs procedures and the control of adult education establishments

warnings are used instead of fines.

The SME 12 / A. § (2), there is no possibility to waive the fine if

(a) the infringement harms or endangers human life, limb or health,

(b) damage to the environment as a result of the facts on which the fine is based

occurred

(c) a legal provision for the protection of persons under the age of eighteen

there has been a breach, or

(d) the infringement is committed on the grounds of age, credulity, mental or physical handicap

particularly vulnerable person in a clearly identifiable group

row,

(e) the undertaking infringes the provisions of the Consumer Protection Act 1997 relating to conciliation proceedings;

year CLV. the obligation to cooperate specified in Section 29 (11) of the Act.

II.2. For data management from 25 May 2018

Pursuant to Article 2 (1) of the General Data Protection Regulation, this Regulation shall apply to:

processing of personal data in an automated way, in whole or in part

for the non-automated processing of personal data which are subject to any of the following:

are part of a registration system or are intended to be part of a registration system

to do.

Under Article 4 (10) of the General Data Protection Regulation, a third party is a natural person

or a legal person, public authority, agency or any other body which is not the same

with the data subject, the controller, the processor or the persons who are the controller

or have been authorized to process personal data under the direct control of a data processor.

Processing of personal data under Article 6 (1) of the General Data Protection Regulation

lawful only if and to the extent that at least one of the following is met:

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

purposes

treatment;

13

(b) processing is necessary for the performance of a contract to which one of the parties is a party; or

to take steps at the request of the data subject before concluding the contract

required;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) the processing protects the vital interests of the data subject or of another natural person

necessary;

(e) the exercise of a public interest or the exercise of official authority vested in the controller

necessary for the performance of its task;

(f) processing is necessary for the protection of the legitimate interests of the controller or of a third party,

unless those interests take precedence over the interests or essential interests of the data subject

rights and freedoms which require the protection of personal data, in particular where

affected child.

Collection of personal data pursuant to Article 5 (1) (b) of the General Data Protection Regulation

only for specific, clear and legitimate purposes and should not be treated for those purposes

in an incompatible manner.

According to Article 5 (1) (c) of the General Data Protection Regulation, personal data are:

they must be appropriate and relevant to the purposes of the data processing and necessary

should be limited (‘data saving’).

Pursuant to Article 5 (2) of the General Data Protection Regulation, the controller is responsible for

shall be able to demonstrate such compliance

(“Accountability”).

Infotv. Pursuant to Section 61 (1) a) in the data protection authority proceedings

the Authority with the data processing operations specified in Section 2 (2) and (4)

in this context, the legal consequences set out in the General Data Protection Regulation

you can apply.

Pursuant to Article 58 (2) (b), (d) and (i) of the General Data Protection Regulation, the supervisory authority condemns the controller or processor, acting in his or her capacity to rectify data, if he or she is a data controller infringed the provisions of the Regulation or administrative proceedings in accordance with Article 83 shall impose fines on the measures referred to in this paragraph, depending on the circumstances of the case in addition to or instead of them.

Pursuant to Article 83 (5) of the General Data Protection Regulation, the principles of data processing, including Articles 5, 6, 7 and 9 of the General Data Protection Regulation in accordance with Article 83 (2)

With an administrative fine of EUR 20 000 000 and, in the case of undertakings, the previous financial penalty up to a maximum of 4% of the total annual world market turnover for the year, provided that the the higher of the two shall be charged.

III. Decision:

III.1. With regard to data processing carried out before 25 May 2018

III.1.1. Legal basis for data management

Based on the Data Protection Policy of the Debtor used during the period under review, it can be stated that the indicated the consent of the data subject as the legal basis for the data processing presented in it. In his statements however, in addition to arguing that the consent basis is data processing related to access

significant potential as a possible alternative substantiation of a legal basis based on a legitimate interest in the statements received.

The Authority issued NAIH / 2017/3208/13 / V. as set out in its letter of formal notice no meg:

III.1.1.1. The consent

One of the most important components of the validity of the consent2 is the voluntary nature of the will of the data subject, freedom from outside influence, which is achieved when there is a real choice for the data subject

available to you. Where the consequences of consent undermine an individual 's freedom of choice,

contribution is not considered voluntary.

Consent should also be based on adequate information. The appropriate information is on which

through which data subjects learn about the processing of their personal data and the information

through which the right to information self-determination can be exercised: the processing of data may be lawful

its circumstances are fully known to those concerned. The requirement to inform the data subject in advance

Infotv. Section 20 details.

Based on the statements and regulations of Sziget Kft

events, you had to provide all the personal data you requested during admission - that is

essentially meant scanning the identity card - without it it could not have taken part

event. Thus, despite the fact that it can be identified as a separate data management purpose with customer registration and

data management related to access, during which the data is processed according to the statement of the data controller

separated, they were not connected in any way, the purchase of tickets and passes and its

attending an event to be provided in return for a separate event is separate from the one associated with it

the establishment of data management, the consent to be given to the data management related to access

depended.

In view of the above, consent cannot be considered an appropriate legal basis in cases where the consent is

no other independent data management or consideration may be provided without giving it

service used for payment. In the Authority's view, there was therefore no real election

the possibility for data subjects to process data relating to access.

III.1.1.2. Legal basis based on a legitimate interest

Sziget Kft. Did not refer to this legal basis in its Privacy Policy, but in its statements

argued that the processing of visitors' personal data in connection with access was not

constitutes a restriction which is disproportionate to the aims pursued, that is to say, to the lives of the visitors

and the prevention of other abuses. They also highlighted that they did

the application of the developed system, through general and special prevention, is suitable for preventing

or to prevent terrorist acts.

The condition for the application of a legal basis based on a legitimate interest is that the controller has a substantive interest

and provide relevant information on the outcome to those concerned.

The Debtor argued without the existence of a legitimate interest of his own or of the visitors as third parties

in addition to having previously carried out the necessary balancing of interests in any form, which

2 Infotv. Consent according to § 3, point 7: voluntary and firm declaration of the will of the data subject, based on appropriate

information,

and by which he or she gives his or her unambiguous consent to the processing of personal data concerning him or her, in

whole or in part.

it in itself questions the validity of that argument. However, the Authority examined the

Debtor's submissions and the following stated.

III.1.1.2. a) Prevention of abuse of access (economic interest of the controller)

Both the Debtor appeared more strongly at the signal given by the Authority in the previous investigation procedure

in its statements and in the Privacy Policy to prevent abuse of access as

the purpose of the data processing related to access.

In this context, the Authority considers certain to be acceptable, as in the case of an independent data management purpose

processing of personal data on the basis of a legitimate interest of the controller, but only for the processing of such data

may occur in this case, suitable for the purpose, such as a photo and a name

attachment and personalization of the armband through it. The additional data set - citizenship,

the type, number and expiry date, date of birth and non - registration of the identity document do not comply with

the principles of purposeful and necessary data management, so the data management is regulated by Infotv. Section 4 (1) -

(2)

conflicted with paragraphs.

III.1.1.2. b) Ensuring the personal safety of visitors

In general, the Authority also considers it an acceptable goal to ensure the safety of festival-goers.

For this purpose, the economic organization of both the company organizing the event will appear at the same time

the security of both citizens and visitors as third parties in terms of data management.

It is important to emphasize in this regard that among the latter interests - if the Debtor

in accordance with its statements, the actual threat of terrorism or criminal offenses

it is essentially in the public interest for the

validation of which, including the definition of the nature and means of performing the public task

it is not directly his job, accordingly it may be necessary to perform such a task

data does not have the means or legal authority to actually use it for this purpose.

Accordingly, no interests may be invoked in connection with the processing of personal data with which

in relation to which the data controller cannot actually act lawfully, may take measures, ie which data

processing from the point of view of the data controller is in fact considered pointless, since the data are processed by the data

controller

you cannot use it to enforce that interest.

Deciding what threats to the safety of those involved are threatened and what they are

data processing - can be combated effectively using a complex

an issue where the exercise of the right for the purpose is to be considered at the same time is the applicable instrument

- in this case, the suitability and indispensability of the device involved in data processing.

In the opinion of the Authority, Sziget Kft. Is related to admission in the last three aspects

data management did not comply with Infotv. conditions imposed by the

Examination of the necessity (necessity) and adequacy of the applied practice

In addition, the Authority shall amend NAIH / 2017/3208 / V. several Europeans of similar size

he also reviewed the admission practice of the festival and set it as an example to show what it is like

other methods can provide a high level of protection by means of means

the right of data subjects to self-determination is less violated.

In its statement dated 19 July 2017, the Debtor did not sufficiently substantiate why they would not have

other methods may be used during entry. His statement merely contained that presented

solutions are “not automatically applicable” at their events, as their company’s festivals are the ticket

transferable (therefore not necessarily the same as the ticket purchaser and the visitor) with ‘market realities

there are reasons ”.

The Debtor did not substantiate the factors hindering the transposition in the quoted statement.

since it did not shed light on the Authority, nor did it shed any light on the Authority

explained why it would not be possible e.g. to limit the transferability of the ticket at an earlier date, and

personalization in some other way that is less infringing on the data subjects' right to self-determination.

In examining the suitability of the system in place, the Authority concluded that

that the efficiency of the system used is questionable, since the database is armbands

therefore, on the one hand, as the Debtor does not have a so-called

‘Reference database’, ie it cannot compare the recorded data and

was only entered into the database when it arrived at the access gate and was scanned there

the method used casts doubt on the act which he may potentially commit

effective defense if it takes hours to enter the database (after which a few

minutes later in the festival area) and between when the competent authorities detect the danger

and they can take action against it. Not to mention if you enter the festival area with any fake documents

perpetrator, which the Debtor was also unable to detect.

Therefore, the Authority does not consider the chosen tool or method to ensure the safety of visitors

necessary and appropriate to achieve the objective pursued, and the Authority

In his view, the scanning of an identity card and the accompanying one cannot be considered proportionate either

associated with the processing of data. Data management - as a method used -

its inadequacy also means that the processing is therefore not real, lawful

acceptable purpose.

The Authority does not consider consent to be an appropriate legal basis for data processing during access,

moreover, the Debtor did not invoke the legitimate interest in law, therefore the Authority finds that the investigated

In the period, the data management did not have an appropriate legal basis, so the data management did not comply with the Infotv.

The requirements of Articles 5 and 6 against the existence of an appropriate legal basis.

III.1.2. Data retention period

The Authority notes that NAIH / 2017/3208 / V. fulfilling the requirements of No. 1, predominantly the Debtor has amended its Privacy Policy accordingly during the period under review, however, some deficiencies could still be discovered in the regulations, due to which the Infotv. Section 20 (2) information to data subjects, even in respect of whose treatment is otherwise not inherently unjustified.

Thus, the Authority does not consider the duration of data processing to be appropriate in cases where it is the personal data of the data subjects were retained by the Debtor for more than 72 hours after the closing of the festival. Given that the data recorded during admission is beyond 72 hours after the closing of the event According to the Debtor 's statement, the purpose of the proceedings is to initiate a procedure, therefore the The Authority is of the opinion that the retention of data should initiate the procedure and provide the necessary data after being handed over to the competent authority, it was not intended to be notified to the authorities was classified as inventory data management, thus violating Infotv. Section 4 (2).

III.1.3. Information on data management

In addition to the above findings regarding the unlawfulness of data processing, it is significant The Authority assesses that Sziget Kft. did not provide information to the user

data processors and their responsibilities. This is especially infringing in the case where Netpositive Kft. plays a significant role in the data management process.

In view of the above, the Authority finds that the Debtor did not provide during the period under review adequate information for the data subjects, so its data management did not comply with Infotv. § 20 specified requirements.

III.2. With regard to data management from 25 May 2018

The Authority shall, in accordance with Article III.2.1. examined the lawfulness of the processing of the data covered by the

It is mandatory to impersonate the wristbands and manage all accesses by displaying them on the access monitor to avoid

abuse and personalize visitors.

in order to safeguard its security, and in accordance with Article III.2.2. examined those data separately

the lawfulness of the management of the data, which the Controller manages in such a way that it does not display everything

times during logins, but stored on a server and “used” in “exceptional” cases.

III.2.1. Manage personal information to avoid misuse as well as personal visitors

to ensure its safety

The Defendant has conducted a balancing test to verify that visitors are personal

security interest of the Debtor in the safe conduct of the event

and the economic interest of the Debtor in the prevention of abuse

takes precedence over restrictions on the right of visitors to the protection of personal data.

According to the rules of the GDPR, a reference to a legal basis of a legitimate interest is correct if the processing is data

for the benefit of the controller or a third party other than the controller and the data subject

so the interest balancing test is on one side of the balance sheet by the data controller or a third party

the legitimate interest of the data subject (s) must be shown on the other side and the opposite

to establish, after a conflict of interests, that the rights of the data subject are being restricted

proportionate to the legitimate interest of the controller or of a third party in that restriction.

The Authority shall declare at the outset, in relation to the balancing test, that it does not

it is acceptable that in the investigation of the counter-interest of the Obligated Visitors (i.e., Stakeholders) only

noted that “the data subjects' (…) concerns about data processing

in general, as with all data processing, that they do not wish to have their personal data stored,

that is, it did not examine in more detail which rights of data subjects are restricted

data management, the extent of the restriction and the risks involved, if any

means to the data subject, so the Debtor has conflicting interests and restraint

did not consider the legality of the test in the test. Accordingly, in the present proceedings

nor has the Debtor raised any substantive arguments on the basis of its statements

judge why the interests he claims would outweigh the interests of those concerned, his or her third party

why it would be proportionate to restrict the privacy of individual data subjects to the interests of individuals.

Declarations and documents sent by the Debtor, including the balance of interest test, also

- III.2.1.1. and III.2.1.2. as detailed in points 1 to 4, do not demonstrate that the

data management would be suitable for all the data management purposes named in the test, ie

that the processing could be lawful.

III.2.1.1. Data management to prevent misuse

The Authority considers it an acceptable practice for the Debtor to avoid abuse

checks that only the person to whom the

after redemption, the armband was assigned during the first entry.

The Authority also agrees that the Debtor has a legitimate economic interest in

that no more persons can enter with the tickets sold, and that ticket vouchers do not pass on multiple

purchased tickets and to identify the stolen in the event of theft

festival tickets.

In the opinion of the Authority, the Debtor has a legitimate interest in avoiding abuse a

It is considered a significant economic interest of the obligor, which may give priority to visitors

against the right to the protection of personal data, so the restriction is not necessarily disproportionate

in the event that the Debtor handles only the personal data of the visitors which a

to avoid abuses which are necessary for this purpose and which are fit for purpose

to achieve. However, a legitimate interest in the legality of a legal basis as a reference must necessarily apply

it is necessary, in accordance with the above, to properly identify competing interests and

weighting.

the)

Assessing the suitability of data management

As a first step, the Authority examined whether the data processing performed by the Debtor in general

whether the data processing can have any effect on the achievement of the purposes indicated by it a

the activity of ticket guns described above, the identification of stolen armbands, and its

to prevent a purchased and triggered armband from being different in succession

person to enter the festival area.

In the Authority's view, the data processing in question is exclusively a ticketing activity

in which they pre-purchase the ticket, redeem the armband,

then the already redesigned wristband will be resold at a higher price. In the opinion of the Authority

however, in most cases ticket sellers do not resell the wristband that has already been used,

rather, they purchase more tickets in advance (as there is no limit to one person

can only buy one ticket) and the pre-purchased ticket is sold - typically via the internet

- at a higher price, without getting tired of the festival venue, replacing it with an armband,

then the already triggered armband would be sold on site.

In the Authority 's view, given that the personalization of tickets on first entry is

when replacing a ticket with an armband, and not when purchasing tickets - the

data processing is not suitable for the activity of ticket offices as described later

to curb. As the tickets purchased in advance are not for a name but for a show,

Thus, regardless of the entry practice used by the Debtor, it may be certain

a person buys more tickets in advance, which sells tickets in excess of the price as they enter the festival area

the person who presents the ticket at the exchange gate is entitled to enter and not the person who presents the ticket

originally purchased.

Furthermore, in the Authority's view, the data processing is not suitable for curbing theft from the cash register, as the entry

staff will not determine on the basis of

whether the wristband has been stolen, which person wishes to enter it, so the

personal data of the visitor, but only the data identifying the wristband, which are

the Debtor is able to determine whether or not a particular wristband has been sold.

In the Authority's view, it would have been appropriate and sufficient for this purpose by the Debtor earlier

the practice is to record the serial number of the armbands (i.e., which

wristband at which fund and at what time), since in possession of this information

it can be determined if an armband has been stolen, based on the fact that if it is stolen from a cash register, it is out

unspecified armbands became the victim of theft.

19

In view of all this, the data processing performed by the Debtor with regard to the prevention of misuse

alone is suitable to prevent several persons from entering the armband a

The only existing and acceptable purpose of data management in this context is

may filter out and curb abuses such that a purchased ticket

with the same triggered armband, several different people can visit the festival one after the other,

In the other cases mentioned above, the data processing is for no purpose, so the data processing for other purposes is a

Infringement of Article 5 (1) (b) of the GDPR.

b)

The question of the need for a managed data set

In assessing the legality of the practice, the Authority subsequently examined whether

all that is displayed on the access monitors at all times during logins

whether personal data - such as image, name, gender and date of birth - are required to be a Debtor

determine whether the person entitled to enter is in fact intending to enter the festival area, ie

whether it is necessary to know all the data in order to prevent abuses or whether the purpose can be achieved

even with a narrower range of data.

The Authority cannot agree with the Debtor's argument that

is required to be displayed and verified because you may have retrieved it from the visitor's document

based on the image taken on the first day of the festival, the visitor will not be unequivocally identifiable,

and in the presence of this additional data set — name, date of birth, and gender — in case of doubt, the visitor

from the identity of the entry staff can verify the entry with control questions

the identity of the person intending to.

In the Authority 's view, in order to prevent abuse, it is not relevant that:

exactly who is the person who is trying to enter the festival area, but that the

the person wishing to enter and the person assigned to the armband must be the same, and in this respect there is no

significance of that person’s date of birth and gender, as the image on the monitor

and the name must be sufficient for the access staff to establish identity.

The Authority agrees with the Debtor's statement that it is on the identity document

the photograph is not always suitable for identifying the holder of the document beyond doubt,

for example, if the document is very old but can be identified beyond doubt

also that the Debtor takes a photo on the spot of the entrants who have their ID

cannot be clearly identified from the photograph on their document, so the date of birth and

no knowledge required.

Furthermore, in the Authority's view, the Debtor's argument is also incorrect because the other data

its handling is not suitable for establishing identity, as anyone can remember it

three personally identifiable information, so if the access staff is the image shown

cannot determine whether the person wishing to enter is wearing an armband at the time of entry

whether he is entitled to enter will not help to decide whether that person can respond to the

control questions, ie whether you can revoke the gender of the person authorized to enter and

date of birth.

It must therefore be sufficient for the access monitor to be able to identify you during access

the image and name of the person who wants to log in is displayed, which is displayed when

entry staff have doubts about the right to enter, the person intending to enter

may require the presentation of an identity card, as the visitor has no doubt

this method alone is suitable for identification.

In view of all this, in addition to the image and name of the visitors on the access monitor, their gender and

In the Authority 's view, the treatment of the date of birth is neither necessary nor appropriate

prevention of misuse, so that the processing does not comply with Article 5 (1) of the Regulation.

requirements of Article 6 (c) of the Regulation and, consequently, of Article 6 (f) of the Regulation.

cannot be considered lawful either.

III.2.1.2. Data management to ensure the personal security of visitors

In assessing the legality of the practice, the Authority also examined whether the entries

during the personalization of the armbands and displayed on access control monitors

whether all personal data, including image, name, gender and date of birth, are required to

Obliged on the basis of this data management can prevent or deter terrorist acts, respectively

the commission of other violent or drug-related offenses, and that the

whether data management is generally a suitable way to achieve the objectives and, if so, a

Whether the data set managed by the obligor is suitable for this.

In connection with this issue, the Authority will refer back to the above point III.1.1.2. (b), in particular

that the interests identified by the Debtor here are in fact public interest objectives that are enforceable

it is not the duty of the Debtor. This alone would not necessarily do the Debtor's data management

unlawful, but, as will be explained below, that the Debtor

links its data processing to the enforcement of purposes for which it does not itself lawfully have a

by appropriate means, it carries out data processing essentially without a legitimate purpose, since if the interest is given

it is not directly his responsibility to determine the nature and means of performing the public task

the necessary data processing and the actual use of the data for this purpose

have the appropriate privileges. Article 6 (1) (f) of the General Data Protection Regulation

does not provide a basis for the processing of data by reference to interests in respect of which the

the data controller cannot actually act lawfully, take measures, ie which data is processed

from the data controller's point of view.

This does not mean that the legitimacy of the stated objectives is called into question, nor does it mean that

to the extent necessary for a legitimate purpose that can be actually achieved and enforced by the controller

the processing of specific data is indeed necessary, no security considerations should arise (eg

protection of the health and physical integrity of the persons present at the event), but these are provided by the Debtor

may require different interests and different data processing,

they would be judged significantly differently.

However, the Authority recognizes the economic nature of the Obligation to organize safe events

interest, however, in his opinion, the purposes indicated by the Debtor (acts of terrorism, violent

and other drug-related crime)

can only be achieved through cooperation with authorized bodies, not the Debtor himself

may replace eligible public actors.

The Authority even points out that the tasks of the competent public bodies, their performance, and

the related data processing is also regulated by law. The legislature is in question

did not impose any tasks on the organizers of the events in the field of public tasks, thus

to date, it has not enacted legislation to reduce the terrorist threat

would make data processing mandatory for large and presumably larger

musical and dance events, so the terrorist threat was not

the legislator wanted to address this through data management.

The Authority maintains its position expressed in the notice of initiation of the previous investigation procedure,

considers that the objectives set by the Debtor are not primarily those of the

by processing personal data, but by other means - e.g. physical inspection, metal detector,

through cooperation with appropriate security staff, the police and other bodies,

feasible.

There is, of course, no obstacle in principle to addressing the security risks in question

authorities empowered to take the necessary measures to that end

within the framework of the legal rules applicable to them

- in the context of which they themselves carry out data management activities or the event

the organizer or other persons to the extent and to the extent necessary, but in the present case

this is not the case, as the Debtor carries out such data processing without

would be required by law or regulation.

the)

Assessing the suitability of data management

In the light of the above, the Authority has examined the data management to achieve the stated objectives

and found that the practice previously used by the Debtor was not

is suitable for the purpose it has set itself, since the last three years of the investigation

access control system, the most significant and only such official request was made

that the Debtor has one, sometimes two, data per day from the data of the access control system during the event

provided TEK with the birth names and dates of those already admitted. This is the solution

it was obviously not suitable for prevention and screening, as the person posing the danger had long been

he was in the festival area when the information about him became available to TEK.

The Debtor relied on the access practice in proving the lawfulness of the data processing

general preventive nature, ie that data processing during access in general

suitable to reduce the number of named crimes.

The Debtor has not adequately substantiated that the use of the access control system is in any way

would have the effect of reducing the number of criminal offenses and thus did not prove that the

system would be suitable for general prevention in any way.

Press articles cited by the Debtor - citing official BRFK announcements

they only report that the crimes are due to the work of the police

year-on-year, from 2016 to 2017 and from 2017 to 2018,

The press article also does not state that the processing of data during entry will reduce the number of criminal offenses.

would have any effect on its development.

Given that the Debtor is implementing data management in 2016, 2017 and 2018 as well

admission practice, so the data processing during the admission was committed

has not been proven to have an impact on crime, in particular the fact that

The festival had the fewest crimes in 2018, despite the fact that a

Debtor has already handled less data this year than in previous years.

As none of these press articles, nor the BRFK Communication, compare the entry

crime statistics for festivals in the years before and after the application of the system,

Thus, it cannot be established that the access control system reduced the

number of criminal offenses, ie the Debtor has not duly demonstrated that the data processing is appropriate

would be the stated purpose of data processing - ie terrorist offenses and other criminal offenses

to achieve this.

Given that the Debtor does not use any algorithm to determine

which person may be a potential perpetrator of a particular crime and that he or she may not

does not have access to any records, so at the time of enrollment you do not yet have information on

which person is likely to commit the offense, so in the Authority's view the

the processing of personal data - ie the data processing itself - is not suitable for terrorist acts,

and the prevention and repression of other criminal offenses.

Furthermore, the Authority is of the opinion that data processing is not intended to curb crime either

may be appropriate, as the Debtor will only be aware during the application of the access system that

who is in the festival area, however - only the application of the check-in system

as a result - unable to establish who committed the crime in the festival area

committed. The identity of the offender using data processed as a result of the practice used a

A debtor can only establish if he is in the act of committing a criminal offense

identifies the perpetrator and identifies him on the basis of the information extracted from his armband, this data processing

however, it is not necessary at all, as in the event of an accident, the Debtor or the competent authority

may require that person to prove his or her identity.

In view of the above, the Authority is of the opinion that data processing could only be envisaged

is suitable for the purpose specified by the Debtor, provided that it is handed over by the competent authority

a list of persons who are past or potential future

offenders, persons posing a danger who should be prevented from entering the festival

and to notify the law enforcement agencies, so if the Debtor had a so-called reference database, however, it did not take place

at any of the festivals held in 2018

upon official request. In this case, however, the data is already actually processed by that authority

would be a data processing activity in accordance with the provisions of that authority, where

the purpose of the data processing would not be determined by the Debtor either.

The Authority is of the opinion that terrorist acts, other acts of violence or drugs

in the prevention and deterrence of criminal offenses, it is irrelevant that

exactly who is the person who is trying to enter the festival area, but that the

whether the person wishing to enter is a person indicated by the authority to the Debtor

and the date of birth of that person is irrelevant in that regard

gender, as the image and name on the monitor must be sufficient to

entry staff should screen the person in question and, where appropriate

ask you to prove your identity. If the visitor arrives with a genuine document,

can properly identify himself, and if the document he has is false, the data extracted from it

are also fictitious, so data management will not be able to achieve the goal in that case either.

The processing of data by the Debtor in the manner examined - in the name and on behalf of the person entering

In the case of data beyond the image, it is of a stock nature and is defined as above

cannot serve a data management purpose, is not suitable for the purpose.

Under the principle of accountability, it is the responsibility of the controller to prove that it is his

the data processing used complies with the principles set out in the Regulation and is therefore obliged, inter alia, to do so

duly demonstrate that its data processing complies with the purpose limitation and data protection principles,

however, the Debtor could not prove this.

In view of the above, the Authority found that during the period under review personal data

without a specific legitimate purpose and therefore does not comply with Article 5 (1) of the GDPR

(b).

As the data management applied by the Debtor is generally not suitable for the purposes indicated by him

and because the Debtor did not rely on it in its balancing test

the conditions for the application of the legitimate interest basis, as the interests of the persons concerned are not at all

identified, so that no actual consideration was actually made, the data management does not comply with the

requirements of Article 6 of this Regulation.

23

III.2.2. Judging the lawfulness of other data processing purposes

The Debtor shall, after reading from the identity document, but without copying the document, record the

the surname and first name, date of birth, country of origin, nationality and sex of the person concerned,

and captures the photograph on the document or, if the photograph is on the document

recording is not possible due to technical reasons, a photograph of the person concerned will be taken on the spot.

The Authority agrees with the Debtor's practice of not displaying the

the country of origin and nationality of the person wishing to enter, as these data are not

they are neither necessary nor suitable for the purposes indicated by the Debtor.

the)

The Authority considers that the country of origin of the visitors is not appropriate - ie

to the issuing authority for the purpose of establishing that:

in the event of a possible terrorist offense or other criminal offense, which country is being represented abroad

shall be notified to the competent authority.

The marked data management is considered to be a repository, as the defined purpose is an uncertain future

event, an exceptional situation which does not occur in the vast majority of cases, thus

the processing of the data on the country of origin of all visitors for this purpose by the Authority

In its view, it does not comply with either the purpose limitation principle or the data - saving principle, so that

data processing is in breach of Article 5 (1) (b) and (c) of the Regulation.

b)

In the Authority's view, it is an inappropriate practice regarding the nationality of the visitor

recording of data where the sole purpose is to commit a terrorist offense or other acts

as a result, the visitor would lose consciousness and subsequently recover or be in a state of shock

the language in which the data subject can be communicated.

In the Authority's view, the processing of data on nationality is not necessary for the stated purpose

because the stated purpose of data processing is still an exceptional situation,

which does not occur in the vast majority of cases, hence the nationality of all visitors

storage of relevant data is considered as inventory data management. The Authority also assumes that:

in most cases, festival-goers from abroad have at least one general

with a minimal level of knowledge of a common foreign language in which to communicate fluently

he can also, but at least he can tell what language he understands or what nationality he is.

In addition, the Authority considers that data processing is not always appropriate for the purpose,

for a “emergency” visitor may be of a nationality that is linguistic

the Debtor does not have an interpreter in any case, in which case the Debtor or other, e.g. given

In this case, the authority acting in the case will presumably try to use it in another language in order to react quickly

communication does not seek interpreters who understand the mother tongue of the data subject

in order to try.

The general suitability of data management is further questioned by the fact that in some countries (e.g.

Switzerland, Belgium) has several official languages, such as a Swiss or Belgian nationality

your nationality is not suitable for determining your mother tongue.

c)

In the opinion of the Authority, the Debtor does not comply with the principle of data saving

nor is it its practice to record the gender of visitors, as it is identification

In addition to the name and image, it is irrelevant whether the person wishing to enter is a woman or a man,

for the purposes of identification, only the fact that the person seeking entry and

the person whose person was assigned to the armband when the ticket was redeemed is the same

whether a person.

In view of all this, the processing of your visitors' gender data is not fit for purpose

nor the principle of data protection, so that data processing is covered by Article 5 (1) (b) of the Regulation.

and (c).

As information on the country of origin, nationality and gender of visitors is not required a

In order to achieve the purposes indicated by the Debtor, the data processing is not suitable for the fulfillment of these

purposes,

Thus, in the Authority 's view, the conditions for the application of a legitimate interest are not met, thus

the personal data of the Debtor regarding the country of origin, nationality and gender of the visitors

without proper legal basis handles the storage of this data, so the management of this data

does not meet the requirements of Article 6 of the Regulation.

III.3 Sanction and justification applied:

III.3.1. With regard to data processing carried out before 25 May 2018

The Authority has established during the clarification of the facts that the Debtor has been in existence since June 2016.

at events organized until the 24th of May

the lack of an appropriate legal basis for the processing of data in connection with access, a

breach of the principle of necessity and of prior information to those concerned

Infotv. Section 4 (1) - (2) and Section 20, and a

The obligor did not comply with the Infotv. Requirements of Sections 5 and 6.

Given that the Debtor's previous data management practices were infringing, it is

data processing has actually been completed, further to the fact that the previous data processing was infringing

the imposition of a fine - in the meantime the legal environment has changed

would not have a significant deterrent effect, it could only be used as repression, a

With regard to the illegal data processing of Sziget Kft. During this period - also taking into account

that a considerable amount of time has elapsed since the dates of the events covered by these data

waived the application of the fine.

The question of whether the Authority is entitled to impose a data protection fine had to be taken into account

take the SME. rules: the SME TV. 12 / A. In examining the existence of the conditions set out in § a

The Authority clarified whether it is an obligated small and medium-sized enterprise (SME)

or not.

The SME Pursuant to Section 3 (1), an enterprise that has all its employees is an SME

has a staff of less than 250 and a net annual turnover of up to EUR 50 million

the amount of HUF or the balance sheet total does not exceed EUR 43 million.

According to the Debtor's annual report for 2017, the average number of employees is 104

main, sales revenue was HUF 1,253,917,000, ie Kvvtv. qualifies as an SME within the meaning of

On the basis of all this, the Authority would not have been entitled to impose a fine on 25 May 2018

due to unlawful data processing carried out prior to

III.3.2. With regard to data management from 25 May 2018

25

The Authority has established that in the course of its data processing as of 25 May 2018, the Debtor

infringed Article 5 (1) (b) and (c) of the Regulation and

and Article 6 of the Regulation. However, with regard to this infringement, the Authority a

considered it appropriate to impose a fine as follows.

As to whether the imposition of a data protection fine is justified, the Authority

Article 83 (2) of the Data Protection Regulation and Infotv.75 / A. § considered ex officio

all the circumstances of the case and found that, in the case of the infringement found in the present proceedings,

the warning is neither a disproportionate nor a dissuasive sanction, so a fine should be imposed.

Given that the GDPR does not contain a derogation from its rules on fines

provisions for SMEs, so that the Authority can impose fines

did not take into account the SME. provisions.

As to whether the imposition of a data protection fine is justified, the Authority

(2), it considered all the circumstances of the case. The Authority considers it necessary to impose a fine

because the Debtor has an inappropriate legal basis, purpose and data protection

treated the personal information of hundreds of thousands of visitors in violation of its principles.

In view of this, the Authority Pursuant to Section 61 (1) (a), in the operative part

and in this decision to pay the data protection fine to the Debtor

obliged.

The amount of the fine was determined by the Authority acting in accordance with its statutory discretion.

Based on the nature of the infringement - lack of an appropriate legal basis, breach of principles - the maximum amount of the

fine that can be imposed

limit of EUR 20 000 000 under Article 83 (5) (a) of the GDPR and, in the case of the Debtor,

not more than 4% of the total worldwide turnover in the preceding business year, whichever is the higher.

In imposing fines, the Authority took into account the following factors as aggravating circumstances:

-

the number of stakeholders, as VOLT, Balaton, organized by the Debtor during the year 2018

A total of more than eight hundred thousand people attended the Sound and Island Festival;

-

the intentional nature of the infringement, since the Debtor in the balancing test

nevertheless related to terrorist acts and other acts of violence and drugs

the prevention and deterrence of criminal offenses was indicated by the Authority

investigation procedure has repeatedly expressed the need for data processing for these purposes

does not find a suitable means of achieving it;

-

the Obliged to play a key role in the market of festivals and entertainment mass events

the assessment of its conduct is of particular public interest and other market participants

can also serve as a model for

-

the fine imposed will be able to achieve its purpose if its amount - the Obliged sales

compared to its sales revenue.

In imposing the fine, the Authority took into account as an attenuating circumstance the fact that the

The Authority has partially complied with its previous request, as it no longer handles the

personal data and no longer scans the entire data content of the identity document,

but reads a narrower range of data from the document.

26

The Debtor cooperated with the Authority during the official proceedings and the inquiries of the Authority

respectively responded on time, although this conduct - due to legal obligations

did not go beyond compliance - was not assessed by the Authority as an attenuating circumstance.

In view of the above, as well as the fact that the sales revenue of the Debtor in 2017

According to the report, it was HUF 1,253,917,000, the data protection fine imposed is appreciable, but

does not exceed the maximum fine that may be imposed.

The Authority shall inform Infotv. Pursuant to Section 61 (2) (a), the Decree shall be ordered by the Debtor Identifier

disclosure of data by a wide range of persons

touch.

ARC. Other issues:

Infotv. Enforcement of the right to the protection of personal data pursuant to Section 60 (1)

In order to do so, the Authority may initiate ex officio data protection proceedings. The data protection authority

CL of the General Administrative Procedure Act 2016. Act (hereinafter: Act)

shall apply with the additions specified in the Information Act.

The Ákr. Pursuant to Section 103 (1) of the Act, ex officio proceedings procedures initiated upon request

The relevant provisions of Art. 103–105. With the exceptions contained in §.

Infotv. Pursuant to Section 38 (2) and (2a), the Authority is responsible for the protection of personal data,

and the exercise of the right of access to data in the public interest and in the public interest

control and facilitation. In the General Data Protection Regulation for the supervisory authority
established entities and entities under the jurisdiction of Hungary
as defined in the General Data Protection Decree and the Information Act a
Authority exercises. The competence of the Authority extends to the entire territory of the country.
Infotv. Pursuant to Section 61 (2), the Authority may order its decision - the data controller or the
disclosure of the identity of the data controller, if the decision
affects a wide range of persons or the seriousness of the infringement has occurred
justifies.
Infotv. 75 / A. § according to Article 83 (2) - (6) of the General Data Protection Regulation
shall exercise the powers set out in paragraph 1, taking into account the principle of proportionality, in particular:
whether it is mandatory under the law on the processing of personal data or the European Union
in the case of a first-time breach of the requirements set out in its legal act
in accordance with Article 58 of the General Data Protection Regulation
by alerting the controller or processor.
The decision is otherwise based on Ákr. Sections 80 and 81 shall apply.
The Ákr. § 112 and § 116 (1) and § 114 (1), respectively
there is an administrative remedy against him.
The rules of administrative litigation are laid down in Act I of 2017 on the Procedure of Administrative Litigation (a
hereinafter: Kp.). A Kp. Pursuant to Section 12 (2) (a) by decision of the Authority
The administrative lawsuit against the court falls within the jurisdiction of the court Section 13 (11)
the Metropolitan Court has exclusive jurisdiction.
Act CXXX of 2016 on Civil Procedure. Act (hereinafter: Pp.) - the Kp. Section 26 (1)
applicable pursuant to § 72 of the General Court in a lawsuit falling within the jurisdiction of the General Court
27
representation is mandatory. Kp. Pursuant to Section 39 (6), unless otherwise provided by law, a
the filing of an application does not have suspensory effect on the entry into force of the administrative act.

A Kp. Section 29 (1) and with this regard Pp. Applicable in accordance with § 604, electronic

CCXXII of 2015 on the general rules of public administration and trust services. Act (a

hereinafter referred to as the Customer's legal representative pursuant to Section 9 (1) (b) of the E-Administration Act

obliged to communicate electronically.

The time and place of the submission of the application is Section 39 (1). The trial

Information on the possibility of requesting the maintenance of the It is based on § 77 (1) - (2). THE

the amount of the fee for an administrative lawsuit in accordance with Act XCIII of 1990 on Fees. Act (hereinafter:

Itv.) 44 / A. § (1). From the advance payment of the fee, the Itv. Section 59 (1)

and Section 62 (1) (h) shall release the party initiating the proceedings.

The Ákr. Pursuant to Section 135, the debtor is entitled to a late payment supplement equal to the statutory interest

is obliged to pay if it fails to meet its obligation to pay money on time.

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

in the case of the debtor, the calendar half-year affected by the delay from the date of the delay

is obliged to pay default interest equal to the central bank base rate valid on the first day of

Budapest, May 23, 2019

Dr. Attila Péterfalvi

President

c. professor