Case number: NAIH/2019/55/5.

Re: Investigation into the data processing conducted at events organised by Sziget Zrt. in connection with admission

DECISION

The Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information, hereinafter: the Authority) brings the following decision in the course of the official data protection procedure launched ex officio concerning the investigation of compliance with data processing requirements by **Sziget Kulturális Menedzser Iroda Zártkörűen Működő Részvénytársaság** (registered office: 1033 Budapest, Hajógyári-sziget, property lot number 23796/58, trade registry number: 01-10-049598; hereinafter: the Obligee), and its *legal predecessor,* conducted at events organised in the period from 2016 to *24 May 2018* related to admissions pursuant to Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act), and data processing conducted at *events organised after 25 May 2018* related to admissions pursuant to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter: GDPR):

1. The Authority **establishes** the unlawfulness of data processing by the Obligee implemented in the course of the admission practice at events organised in the period from *1 June 2016 to 24 May 2018* as the data processing undertaken by the Obligee in the period under study

a) was not based on an appropriate legal basis,

b) failed to meet the principle of purpose limitation,

c) the data subjects did not receive appropriate preliminary information.

2. The Authority **establishes** the unlawfulness of data processing implemented by the Obligee in its admission practice at events organised following *25 May 2018* as the Obligee processed the personal data of the data subjects

a) not on the basis of an appropriate legal basis,

b) in breach of the principles of purpose limitation and data minimisation

during the period under study.

3. The Authority **orders** the Obligee to align its data processing practice in the course of admissions with the rules of the General Data Protection Regulation.

4. On account of the unlawful data processing conducted by the Obligee at events

organised by it after 25 May 2018, the Authority levies a

data protection fine of
HUF 30,000,000, that is, thirty million forints

payable within 30 days from this decision entering into force.

5. Simultaneously, the Authority **orders** the publication of this decision including identification data in its website.

The Obligee shall notify the Authority of the measures it has taken within 30 days from the expiry of the deadline for launching litigation governing the initiation of review by the court.

The fine shall be payable to the forint account for the collection of centralised receipts of the Authority (10032000-01040425-00000000 Centralised collection account IBAN: HU83 1003 2000 0104 0425 0000 0000). When transferring the amount, reference shall be made to NAIH/2019/55/5. BÍRS.

If the Obligee fails to meet its fine payment obligation when due, it shall pay a penalty for delay. The rate of the penalty for delay is the lawful interest rate equivalent to the base rate quoted by the central bank on the first day of the calendar half-year affected by the delay. In the event of a failure to pay the fine and a penalty for delay, the Authority orders the execution of its decision and the collection of the fine and the penalty for delay as taxes.

There shall be no administrative legal remedy against this decision, but it can be attacked in an administrative lawsuit with a petition addressed to the Fővárosi Törvényszék (Budapest Tribunal) within 30 days from its notification. The petition is to be submitted to the Authority electronically and the Authority will forward it to the court together with the documents of the case. The petition must indicate, if there is a request for holding a hearing. For those who are not subject to full personal exemption from levies, the levy for the court review procedure is HUF 30,000; the lawsuit is subject to the right of prenotation of duties. Legal representation is mandatory in any procedure in front of the Budapest Tribunal.

JUSTIFICATION

I. The course of the procedure and the clarification of the facts of the case

I.1. Antecedents, the investigation by the Authority

Earlier, the Authority conducted investigative procedures under case number NAIH/2016/4278/V. and NAIH/2017/3208/V. to investigate the data processing carried out by the legal predecessor of the Obligee, Sziget Kulturális Menedzser Iroda Kft. (hereinafter: Sziget Kft.).

I.1.1. The legal basis of data processing

The Authority received complaints in relation to the VOLT Festival in 2016; the complainants found the practice applied by Sziget Kft. in the course of admissions injurious, as the identification documents of the guests were scanned upon admission and they failed to appropriately inform the data subjects of the circumstances of data processing, including the purpose and the period of processing the copies of the identification documents and what they are used for.

Based on the Privacy Statement of Sziget Kft. in force during the period under study, Sziget Kft. indicated that data processing in the course of the admission process was separate from data processing in the course of the purchase of tickets; in the course of admission, they scanned the identification documents and read, recorded and stored the following data of the data subjects: *citizenship, name, type, number and expiry of the document, birth date, gender.* At the same time, Sziget Kft. also made video and sound recordings of the data subjects, which they also "recorded, stored and processed".

Point 4 of the Privacy Statement available in June 2016 at the time of the VOLT Festival had the sub-heading "*Identification in the course of the admission process*". Pursuant to this, "*in the course of registration at the venue of the events organised by the Controller, (i.e. assigning the wristband authorising entry to a natural person determined in the course of the admission process) the Controller requests the verification of identity with an identification document with photo. In the course of this, the Controller scans, records, stores and processes the data of the data subject recorded in the identification documents and also makes video and sound recording of the data subject, which it also records, stores and processes."*

Sziget Kft. reserved the right to invalidate the wristband and deny entry to the event, if the data subjects did not give their consent to the above.

In August 2016 (the time of the SZIGET Festival), Sziget Kft. modified its data processing practice, but with respect to the legal basis of data processing it maintained the legal basis stated in the earlier version of the Privacy Statement, Point 1.4., i.e. consent, and extended it to the admission process: "*The legal basis of data processing conducted by the Controller is the informed consent of the data subjects granted by accepting the conditions of registration in the course of buyer registration and by participating in the identification in the course of the admission process*".

In its letter under case number NAIH/2017/3208/V. dated 15 June 2017 (hereinafter: first notice), the Authority notified Sziget Kft. it does not regard the consent of the data subject as an appropriate legal basis for the data processing applied in the course of admission as it was not voluntary.

In its letter of 19 July 2017 written in response to the notice, Sziget Kft. presented that in their view, the data subjects have a genuine choice as they have to subject themselves to the admission practice only if they wish to buy a ticket for the event. In their view, as the purchase of the ticket is not mandatory for the data subject, they are in a genuine situation of choice and so they continue to refer to the consent of the data subjects as the legal basis of data processing for the festivals organised in 2017.

I.1.2. The purpose of data processing

With regard to the *purpose of data processing* associated with the admission system, Sziget Kft. presented that they began designing the system following the terrorist acts in Paris in November 2015 when they decided to apply an admission system where the holder of the wristband is to be named when receiving it. In their view, the mass events of Sziget Kft. – similarly to any other mass event – are exposed to the risk of terror to be taken seriously. They also referred to the fact that "*foreign affairs and foreign representation bodies of various countries warned one after the other that inter alia events similar to the festivals of Sziget Kft. may become targets of attacks in the future*".

They also reported that they maintained contact with the "national security services" and other authorities to help their work. The the admission system is designed to ensure that should any "security service" obtain relevant information on an act under preparation, Sziget Kft. should be able to filter out the persons indicated by the authorities. The operation of the system reveals whether a given person entered the event (based on identification data and the recorded photo), and such a person may also be prevented from entering the event. In their view, taking such precautionary

measures cannot be regarded as disproportionate to the threat as they are necessary means to prevent any threat to the safety, limb or life of the visitors.

They also informed the Authority in their statement that in contrast to the provisions of point 4 of their Privacy Statement, the legal basis of data processing at the VOLT Festival and the Balaton Sound was Section 6(5)(b)[1] of the Privacy Act with a view to protecting the personal safety of the visitors participating in the mass events. As mentioned earlier, the Privacy Statement was modified for the Sziget Festival of 2016 and the legal basis became the consent of the data subjects.

In their view, the protection of the personal safety of the participants of mass events is proportionate to the above restriction of the visitors' right to the protection of their personal data, also in view of the fact that the data recorded upon admission are erased within 72 hours following the event.

In their view, there is no other possibility at festivals for the quick admission of such a large number of people, while also enforcing the objectives detailed above. Sziget Kft. stored the data in their own internal database on their own servers at the venues of the individual events and at their registered offices; the data were records with a passport scanner type 3MAT9000; the system recorded photographic information upon the visitors' entry to the area of the festival, or in the case of old type identification documents, the image of the document.

The data were stored and processed until 72 hours after the official closure of the event, after that they were permanently erased, except if an act took place which warranted the further storage of the data (in such cases the data were stored for a year at most, or if obligated by an authority, they were stored for the period specified by the authority).

They also emphasized that "*Sziget Kft. does not forward the data to third persons and it does not compare them with databases or Wanted lists as it cannot and has no desire to take over the duties of the authorities, but emphasizes this possibility in its external communications to increase the system's restraining power*".

With respect to the Authority's question concerning authorisations to access the data, they presented that the staff of Sziget Kft. carrying out the admissions see the photo recorded for any given wristband, but these employees do not have access to the database and cannot search it.

In the course of the admissions, the document images were not presented to the staff carrying out the admissions, they saw the visitor's photo only. Sziget Kft. used the document images only if the document was suitable for recording the photo (in the case of old type ID cards). Apart from identification upon handing over the wristbands and admission with the wristbands and eventual requests, Sziget Kft. did not use the photos and document images. Only the staff members having the highest level of access authorisation (roughly 20 people) had access to the database, however, only in order to be able to comply with the requests of the authorities.

After the above statements of Sziget Kft., the Authority contacted the Police, the Constitution Protection Office and the Terror Prevention Centre (hereinafter: TEK).

The National Police Headquarters reported on the ad hoc cases of cooperation between local police services and Sziget Kft. and also on whether the police took on any other role in the course of the

---

[1] Pursuant to Section 6(5) of the Privacy Act *"if personal data are recorded with the consent of the data subject, the controller may unless otherwise provided by law process the recorded data without additional separate consent and even after the withdrawal of the consent of the data subject*
a) for the purpose of meeting a legal obligation, or
b) for the purpose of enforcing the rightful interests of the controller or a third party provided that the enforcement of such an interest is proportionate to the restriction of the right to the protection of personal data.
"

festivals organised in their areas of competency. They also informed the Authority that they did not request data from the database processed by Sziget Kft., but sent several queries to Sziget Kft. in relation to their own investigations. In addition, they explained that from a professional point of view, they regarded the measures taken by organisers of events attracting large masses of people, which increase the safety of the participants as supportable provided that data subjects are informed of the conditions of data processing, thus in particular of the purpose and period of the processing of their personal data and they made an informed decision whether to buy tickets.

The Constitution Protection Office reported that they did not request personal data from Sziget Kft. with reference to risks to national security, but they support the development of a uniform practice of data processing in the course of admissions to similar events, conducted with a view to supporting national security (terror prevention) activities.

TEK informed the Authority of their reconciliations with Sziget Kft. of the forwarding of data to them, its legal basis and data processing. According to their statement, the data requested by them included the birth name, birth place and the time and date of admission of the persons. TEK also reported that they only requested the data of visitors to the Sziget Festival from Sziget Kft., they did not request data from the databases of other festivals organised by them.

In their view, the threat of terror to events with large numbers of participants is higher than that to other events, requiring greater circumspection on the part of the organisers and constituting a greater task even for TEK in the course of carrying out their duties against terrorism as specified by law. However, they emphasised that a system of admissions processing personal data and its operation must comply with the legal regulations applicable to data processing.

In its first notice, the Authority established that in its view the applied practice was neither suitable, nor indispensable for the achievement of the data processing purposes indicated by Sziget Kft., and in view of this, it called upon Sziget Kft. to transform its system and practice of admissions, so as to comply with the legal requirements in force, particularly with respect to verifying the suitability and indispensability of data processing.

In its response dated 19 July 2017, Sziget Kft. submitted that the admission system applied by them – when the identification documents of the visitors are scanned while personalising the wristbands - is suitable and indispensable for the achievement of the data processing purposes. In their view, the prevention of eventual terrorist acts is a purpose in itself where the measures taken by them cannot be regarded as disproportionate. They regard the on-site identification of the visitors as efficient (despite the fact that it is not done in advance), as it can substantially reduce the threat of terror in their opinion. Perpetrators may fear that in the course of the identification and video recording upon admission, they would get filtered out and not permitted to enter the festival. In their view, no other rational solution can ensure this under the circumstances of a festival.

I.1.3. The purpose of data processing

The investigation of the Authority also extended to whether or not Sziget Kft. provided appropriate preliminary information on data processing to the visitors of the festivals during the period under study.

Pursuant to the Privacy Rules then in force, Sziget Kft. as controller separated the following four cases of data processing in relation to the administration of festivals:

1) collected in the course of purchasing tickets;
2) related to sending newsletters;
3) carried out in the course of admission; and
4) data processing within the event related to its organisation.

The data processing related to admissions was according to the rules warranted primarily by the protection of the personal safety of visitors, and secondarily by filtering out any abuses related to admissions.

With regard to all the data processing cases indicated above, Sziget Kft. indicated the consent of the data subject as the legal basis of processing personal data, implying that, for instance, the data subject grants his consent in the course of purchasing tickets by commencing the purchasing process, while in the case of identification in the course of the admission process by participating in it.

When assigning the wristband authorising admission for a specific natural person in the course of the admission process, the Controller requested the verification of personal identity with an identification document with photo. According to the rules, compliance was a precondition to participating in the event, hence in their view the data subject gave its express preliminary and voluntary consent to the processing of their personal data by the Controller upon admission to the festival.

Furthermore, the Controller informed the data subject that in the event of being obligated by legal regulation or the courts or other authorities, it may forward the personal data of the data subjects or make them accessible or link them via other data processing as stipulated for the person(s) specified therein.

According to the information, the processed personal data of the data subjects were erased by Sziget Kft. after 72 hours following the official closure of the event where they were recorded, except if a well-grounded suspicion of abuse arose, or an act threatening or endangering the life, limb or health of the participants took place. In such a case, the data were kept for more than 72 hours, but at most for a year, or if an authority required otherwise, for the period specified by that authority.

In its first notice, the Authority established that the information provided on the data processing under study did not comply with Section 20(2) of the Privacy Act in force in the period studied by the investigative procedure, and therefore called upon Sziget Kft. to align its information with the provisions of the law and its data processing practice to be reviewed from other aspects.

As Sziget Kft. failed to comply with the provisions of the first notice, the Authority repeatedly called upon Sziget Kft. to review its data processing practice and to transform it in accordance with the legal regulations in force, and to transform its admission system so as to comply with the legal requirements in force, particularly with respect to the appropriate legal basis of data processing in a letter dated 20 December 2017, in which Sziget Kft.'s response of 19 July 2017 was also taken into account.

The Obligee received the notice of 20 December 2017 on 4 January 2018 and submitted a request for extending the deadline by 60 days on 11 January 2018; the requirements set forth in the notice were not complied with until the launching the administrative procedure under the above case number.

I.2. Process of the Authority

Following the above antecedents, the Authority received a complaint on 16 July 2018, in which the complainant presented that copying the identification document of the persons wishing to be admitted to the VOLT Festival organised in June 2018 was a precondition to admission.

In view of the above, the Authority launched an administrative procedure ex officio on 8 October 2018 to investigate

a) compliance of the data processing by the Obligee related to admissions to events organised in the period from 2016 *to 24 May 2018* (essentially the data processing studied in the earlier investigative procedure) with the Privacy Act, and

b) compliance of the data processing by the Obligee related to admissions to events *organised after 25 May 2018* with the General Data Protection Regulation.

As on 31 December 2017, Sziget Kft. was transformed into a privately held company, thus the Authority launched its administrative procedure against Sziget Kulturális Menedzser Iroda Zártkörűen Működő Részvénytársaság.

I.2.1. The framework of data processing related to admissions

In its letter of 25 October 2018 sent in response to the order of the Authority asking for data, the Obligee submitted that it met the requirements set forth in the notice sent under the earlier investigative procedure, it reviewed and transformed its data processing practice, but failed to notify the Authority thereof "for administrative reasons".

The Obligee submitted that it applied the same practice at the major festivals it organised, including the Sziget Festival, the VOLT Festival and the Balaton Sound Festival (hereinafter jointly referred to as: festival) in the course of admissions, thus the statements made by it should be understood as applicable to all three festivals.

The Obligee submitted that the condition of entry to the festival is the personalisation of tickets, which is done as follows: the Obligee records *the first name and surname of the visitor, his birth date, country of origin, nationality and gender,* reading them from the identification document (without copying the document) in the case of a pre-purchased ticket on site at the point of exchange, and in the case of on-site ticket purchase at the on-site cash desk and records the *photo* on the document or if that is not possible for technical reasons takes a photo of the data subject on site.

Exchanging the wristband, the Obligee assigns the personal data of the visitor, as well as his authorisations (which are the days when he is authorised to enter the festival area, which camping he is authorised to enter) to the wristband using the so-called RFID chip on the wristband, which is the electronic identifier of the wristband.

After this, the RFID chip is read every time a person enters through the admission gates, whereby the Obligee checks at every single admission whether the visitor is authorised to enter the festival area (whether his ticket is valid for the given day), and whether the person wishing to enter with the given wristband is really the person assigned to the wristband and authorised to enter.

For the purpose of this checking, the screen in front of the admission personnel at the admission gates displays the the image, name, gender and birth date (i.e. a narrow range of the check-in data) of the person wishing to enter.

Obligee presented that it does not process the copies of documents and the data obtained either from the documents or recorded manually are stored on the server located at the venue of the event and owned by the Obligee but operated by Netpositive Kft., and on the devices located in the Telekom Server Hotel at 1132 Budapest, Victor Hugo utca 18-22.

The Obligee submitted that it erases the data processed by it permanently 72 hours after the closure of the festival at the latest; the Obligee verified the statement by sending the protocols on the data erasure of the 2018 festivals.

I.2.2. Legitimate Interests Assessment by the Obligee

The Obligee submitted that the data processing carried out during admission is done pursuant to Article (6)(1)(f) of the General Data Protection Regulation with a view to filtering out abuses and ensuring the

personal safety of the visitors, thus, both the Obligee has a legitimate economic interest and the visitors have a legitimate interest linked to the processing of the data. To verify its legitimate interest, Obligee sent the Legitimate Interests Assessment (LIA) carried out on 20 March 2018.

The LIA test identifies two sets of interests: the economic interest of the Obligee related to preventing abuses of tickets sold by it and the visitors' interest in life and personal safety, as well as the interest of the Obligee related to the organisation of events which is an indispensable condition to providing a safe environment for the visitors.

a) According to the test, prior to the introduction of the current practice, the Obligee recorded only the serial number of the wristbands (and in relation to this, where and when a wristband was issued), thus it occurred that scalpers bought tickets at the cash desk and then resold them at a higher price. As the ticket was not tied to a person, it could happen that a scalper bought several tickets, redeemed the wristbands and then resold the already redeemed wristbands at a higher price.

According to their statement, it also happened that somebody stole festival tickets from the cash desk and entered the festival with these stolen tickets, but the Obligee was unable to identify the stolen tickets.

It also happened quite frequently that several persons entered one after the other with a single wristband because the wristbands of the visitors no longer in use were bought by scalpers and then resold by them.

b) The LIA test briefly summarises the terrorist attacks committed in the years 2015-2017, on the basis of which the Obligee established that the terrorist threat was genuine and musical festivals, such as the Balaton Sound, VOLT and Sziget festivals organised by the Obligee attracting a large number of visitors, were potential targets of such attacks.

It was on that basis that the test identified the right of festival goers to life and personal safety, which according to the Obligee are fundamental human rights.

According to the test, the physical examination of visitors upon admission is not in itself suitable to achieve the purpose because the festivals are organised in areas, which are open to anyone during the rest of the year, thus in the given case any "instruments against life and personal safety" can be hidden in the area of the festival in advance and as these areas are not controlled by the Obligee throughout the year, it is impossible for the Obligee to fully search them.

The test includes that data processing constituting the subject matter of the procedure together with the physical safety measures are necessary to identify "potential perpetrators".

In relation to this, the test details that the prevention of a terrorist act may in the given case depend on whether the Obligee is able to monitor that persons indicated by the authorities have entered or attempted to enter the area of the festival.

The test also states that the practice applied may serve to filter out not only terrorist acts but also "the potential perpetrators of violent or drug-related crimes".

According to the LIA test, this practice serves not only as special but also as general prevention because it may have a restraining force for anyone, who might plan to commit the above acts.

According to the tests, it is necessary to assign the specified data to the wristband also because experience shows that festival participants do not keep their identification documents on them in the days following admission.

The Obligee examined in its LIA test what rights and interests of the data subjects are restricted due to the admission system. In the Obligee's opinion, it can be stated in general that that data subjects do not want to have their data stored and processed.

The LIA test states that the personal data of the visitors are held by the Obligee during the period of the festival and the 72 hours following its closure as mentioned above, and after 72 hours following the closure of the event they are permanently erased or anonymized.

Other than checking the authorization to enter, the personal data are not used and the Obligee does not link them to other data.

According to the test, the method applied provides psychological protection to the visitors, going beyond the physical protection applied for a long time in practice, because the short-term storage of the data enables the prevention of terrorist acts and other criminal acts in the event of any suspicion arising through the information obtained from the database.

According to the test, the admission practice is favourable also because by applying it, admission takes place faster, long queues are not formed at the admission gates and according to the Obligee, a smaller mass of people is a less attractive target for potential perpetrators.

Because of these arguments, the Obligee believes that the visitors' interest in personal safety and the Obligee's interest in preventing abuse are interests which enjoy priority over the visitors' right to the protection of their personal data.

The Authority had additional questions in relation to the content of the LIA test, which the Obligee answered in a letter dated 18 January 2019 responding to the question of the Authority posed in a new order of the Authority sent with a view to clarifying the facts of the case.

Answering the Authority's question, the Obligee stated that it did not apply any special algorithm and has no access to any registry on the basis of which it could filter out persons posing a threat. They also stated that they decide which person means potential threat based on indications by the authorities and they find the application of the admission system necessary with a view to filtering out persons named by the authorities. The Obligee underlined in its response that they do not use the database to establish the range of persons who potentially pose a danger.

The Obligee stated that the number of criminal acts in question declined steadily following the implementation of the system. The Obligee verified this statement with the professional opinion given by In-Kal Security Events Kft. (hereinafter: In-Kal) dated 17 August 2017 and the articles published in these websites https://nepszava.hu/1137942_iden-a-magyarok-hoztak-a-sziget-nyereseget, https://hvg.hu/itthon/20180815_Joval_kevesebb_buncselekmeny_tortent_a_Szigeten_mint_tavaly, https://www.vg.hu/kozelet/kozeleti-hirek/visszaesett-a-buncselekmenyek-szama-a-szigeten-1049502/ and the official communication of the police on the website http://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/szervezeti-hirek/sziget-iden-kevesebb-buneset-a-fesztivalon.

All the articles report on the communications by the Budapest Police Headquarters (hereinafter: BRFK): the Népszava article writes about the Sziget Festival in 2017, reporting that the number of criminal acts at the festival of 2017 was 16% less than at the festival of 2016; the articles in the websites of HVG and Világgazdaság report on the festival of 2018, announcing that the number of criminal acts in that year was 51% less than in 2017.

All the articles, as well as the BRFK communication praised the work of the police, stating that they participated in the implementation of security with hard work both in the external venues and the

internal area of the festival; none of the articles write about the admission practice applied by the Obligee, its necessity, suitability and impact on changes in the number of criminal acts.

In the profession opinion provided by In-Kal, managing director Dr. Kázmér Lovas explains that the so-called “check-in” system improved the general security of the events of the Obligee with unexpected efficiency and success because in his view, the appearance of undesirable “guests” and the presence of “dealers” declined substantially because of the presence of the system, while minor misdemeanors disappeared almost fully.

I.2.3. The range and necessity of data processed by the Obligee in relation to admissions

With regard to the range of the processed data (first name, surname, date of birth, country of origin, nationality, gender and photo), the Obligee stated that this is a narrower range of data relative to its former practice, as they no longer record the type of document, the authority issuing the document, the expiry and identification number of the document.

The Obligee stated that processing all the data indicated was necessary in order to be able to clearly and doubtlessly identify any person attempting or committing any abuse or threatening or endangering security.

a) In their letter dated 18 January 2019 responding to the Authority’s question posed in its recent order sent to clarify the facts of the case, the Obligee stated that it is insufficient to have only the photo of the person intending to enter displayed on the monitor in front of the admitting personnel for establishing whether or not this person is authorised to enter.

The Obligee justified this statement by saying that it frequently occurs that the image obtained from the identification document of a given person is not fully in line with the current look of the given person and it happens that a person having a weekly ticket will look different on the last day relative to the photo made of him on the first day of the festival.

According to the Obligee, the admission monitor needs to display the name, birth date and gender of the visitor in addition to his photo because in this way the admitting personnel can be assured of the identity of the person wishing to enter through posing checking questions in a manner that excludes any doubt.

b) The Obligee also stated that in view of the large number of foreign visitors, recording the country of origin of the visitors (i.e. the authority issuing the given document) is necessary to enable them to discern which embassy should be notified in the case of an eventual terrorist act or other criminal act.

c) The Obligee stated that recording the nationality or citizenship is necessary to know what language is to be used for communicating with him should a visitor lose consciousness because of a terrorist act or other act and come to thereafter or be in a shock.

In their letter dated 18 January 2019 responding to the Authority’s question posed in its recent order sent to clarify the facts of the case, the Obligee emphasised in relation to this set of data that generally these data are not retrieved, they are not displayed on the monitor upon admission and they only access these data in extraordinary and warranted cases.

Responding to the Authority’s question, the Obligee stated in its letter that volunteers capable of interpreting in English, German, French, Dutch, Spanish, Slovakian, Czech, Russian, Ukrainian, Italian, Turkish and Hebrew languages were available during the 2018 festival season.

II. Legal regulations to be applied in the case

In view of Section 15(1)(a) and (2)(a) of Act CXXX of 2010 on Legislation (hereinafter: Legislation Act), the Authority examined the lawfulness of data processing in the course of its procedure based on the legal regulation in force at the time of the implementation of the data processing operations constituting the subject matter of the procedure, and as it cannot be separated from the substantive legal obligations constituting the basis, it decided on the legal consequences by applying the same regulations. With regard to the procedural rules applicable to the procedure of the Authority, the legal regulations in force at the time of launching the procedure are to be applied in view of Section 15(1)(b) of the Legislation Act.

II.1. Data processing conducted from 2016 to 24 May 2018

Pursuant Section 4(1) of the Privacy Act, personal data shall be processed only for clearly specified and legitimate purposes in order to exercise certain rights and fulfil obligations. The purpose of processing shall be met at all stages of data processing; data shall be collected and processed fairly and lawfully.

Pursuant to Section 5(1) of the Privacy Act, personal data may be processed, if
a) the data subject has given his consent to it, or
b) it is prescribed in an act, or based on the authorisation of an act within the limit set forth therein in a local government decree for purposes in the public interest (hereinafter: mandatory data processing).

Pursuant to Section 6(1) of the Privacy Act, personal data may also be processed, if obtaining the consent of the data subject is impossible or would involve disproportionate costs, and the processing of the personal data
a) is necessary for meeting a legal obligation of the controller, or
b) it is necessary to enforce the legitimate interests of the controller or a third person and the enforcement of this interest is proportionate to the restriction of the right to the protection of personal data.

Pursuant to Section 4(2) of the Privacy Act, only personal data that are essential and suitable for achieving the purpose of processing may be processed. Personal data may be processed only to the extent and for the period of time necessary to achieve its purpose.

Pursuant to Section 20(1) of the Privacy Act, the data subject shall be notified prior to the commencement of data processing whether data processing is based on consent, or it is mandatory.

Pursuant to Section 20(2) of the Privacy Act, the data subject shall be clearly informed in detail of all the facts related to the processing of his data, prior to the commencement of data processing, thus in particular of the purpose and legal basis of data processing, the person authorised as controller or processor of the data, the period of processing the data, of whether the controller processes the personal data of the data subject pursuant to Section 6(5) and of who can have access to the data. The information shall extend to the data subject's rights related to data processing and the legal remedies.

According to Section 61(1)(a) and (g) of the Privacy Act in force during the first phase of data processing (i.e. prior to the entry into force of GDPR), the Authority may inter alia establish the fact of the unlawful handling or processing of personal data in its decision brought in a data protection procedure of the Authority and it may levy a fine, whose extent may extend from a hundred thousand forints to twenty million forints.

Pursuant to Section 3(1) of Act XXXIV of 2004 on Small and Medium-Sized Enterprises and supporting their development (hereinafter: SME Act), an undertaking qualifies as an SME, whose
a) total number of employees is less than 250, and
b) annual net sales expressed in Hungarian forints is equivalent to 50 million euros at most, or balance sheet total expressed in Hungarian forints is equivalent to 43 million euros at most.

Pursuant to Section 12/A(1) of the SME Act, organs performing administrative supervision shall apply a warning instead of levying a fine in the event of a breach of the law taking place for the first time in the case of small and medium-sized enterprises, except for the procedures of the tax and customs authority and the procedure aimed at supervising institutions pursuing adult training activities.

Pursuant to Section 12/A(2) of the SME Act, it is not possible to waive a fine, if
a) the breach of the law endangers or threatens human life, limb or health,
b) the facts of the case serving as the basis for levying a fine caused damage to the environment,
c) a legal regulation aimed at the protection of persons below the age of eighteen years was breached, or
d) the violation of the law took place against a person belonging to a clearly identifiable group of persons, who are particularly vulnerable on account of their age, gullibility, mental or physical handicap,
e) the undertaking fails to comply with its obligation to cooperate in a procedure of a conciliatory body as specified in Section 29(11) of Act CLV of 1997 on Consumer Protection.

II.2. Data processing conducted from 25 May 2018

Pursuant to Article 2(1) of the General Data Protection Regulation, this regulation applies to the processing of personal data wholly or partly by automated means, and to the processing of personal data by non-automated means which form part of a filing system or are intended to form part of a filing system.

Pursuant to Article 3(10) of the General Data Protection Regulation, third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and person who under the direct authority of the controller or processor are authorised to process personal data.

Pursuant to Article 6(1) of the General Data Protection Regulation, the processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
a) the data subject has given consent to the processing of his personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

Pursuant to Article 5(1)(b) of the General Data Protection Regulation, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner that is incompatible with those purposes.

Pursuant to Article 5(1)(c) of the General Data Protection Regulation, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation").

Pursuant to Article 5(2) of the General Data Protection Regulation, the Controller shall be responsible for and able to demonstrate compliance with paragraph (1) ("accountability").

Pursuant to Section 61(1)(a) of the Privacy Act, in its decision adopted in its procedures for data protection, the Authority may apply the legal consequences specified in the General Data Protection Regulation concerning the data processing operations specified in Sections 2(2) and (4).

Pursuant to Article 58(2)(b), (d) and (i) of the General Data Protection Regulation, the supervisory authority acting within its corrective powers may issue reprimands to a controller or a processor, where processing operations have infringed provisions of this regulation, or it may impose an administrative fine pursuant to Article 83 in addition to or instead of measures referred to in this paragraph depending on the circumstance of each individual case.

Pursuant to Article 83(5) of the General Data Protection Regulation, infringements of the basic principles for processing, including conditions for consent pursuant to Articles 5, 6, 7 and 9 shall be subject to administrative fines in accordance with Article 83(2) of up to EUR 20,000,000 or in the case of an undertaking up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

III. Decision:

III.1. Data processing carried out prior to 25 May 2018

III.1.1. The legal basis of data processing

The Privacy Rules of the Obligee used in the period under study reveals that it indicated the consent of the data subject as the legal basis of processing presented therein. In its statements, however, in addition to arguing for the applicability of the consent as legal basis in the case of processing related to admission, the substantiation of the legal basis of legitimate interest as a possible alternative was given substantial emphasis.

Similarly to the provisions of its notice of NAIH/2017/3208/13/V. the Authority establishes the following:

III.1.1.1. Consent

One of the most important components of consent[2] validity is voluntariness of the will of the data subject and exemption from external influence, which is realised if the data subject has a genuine choice. If the consequences of the consent undermine the individual's freedom of choice, consent does not qualify as voluntary.

Also, consent must be based on *appropriate information.* Appropriate information is provided, if the data subjects become acquainted with the processing of their personal data and it is through this information that the right to informational self-determination can be enforced: data processing is lawful

[2] Pursuant to Section 3 point 7 of the Privacy Act, *consent means any freely given specific, informed and unambiguous indication of the data subject's wishes, by which he signifies agreement to the processing of his personal data by a statement or a clear affirmative action.*

provided its circumstances are fully known to the data subjects. Section 20 of the Privacy Act details the requirement of the preliminary information of the data subject.

The statements and rules of Sziget Kft. reveal that whoever wish to participate in the events organised by them had to provide all their personal data requested in the course of admission, which essentially meant the scanning of the identification document without which he could not participate in the event. In spite of the fact that data processing related to buyer registration and admission can be identified as separate data processing purposes, in the course of which the processed data were separated according to the statement of the Controller and they were not in any way connected, the purchase of the ticket and the visit to the event provided as its counter service depended on a separate data processing act when granting consent for data processing related to the admission.

Based on all this, consent cannot be regarded as an appropriate legal basis in a case when without granting consent, another independent data processing cannot be realised, or the service paid for cannot be used. According to the position of the Authority, the data subjects did not have a genuine choice in the course of the processing of their data in relation to the admission.

III.1.1.2. Legal basis related to legitimate interest

In its Privacy Rules, Sziget Kft. did not refer to this legal basis, but it regularly argued in its statements that processing the visitors' personal data in connecton to admissions did not constitute a restriction of such an extent that would not be proportionate to the goal to be achieved that which is the protection of the visitors' right to life and the prevention of other abuses. In addition, they underlined that the application of the system developed by them was suitable by way of general and special prevention to prevent the perpetration of terrorist acts.

The precondition to applying legitimate interest as a legal basis is that the Controller carries out an assessment of the interests in merit and provides adequate information of the results thereof to the data subjects.

The Obligee argued for its own legitimate interests and those of the visitors as third persons without having conducted the necessary interest assessment in advance in any form whatsoever, which in itself questions the grounds of such an argumentation. Nevertheless, the Authority examined what was submitted by the Obligee and established the following.

III.1.1.2. a) Prevention of abuse in connection with admission (economic interest of the Controller)

Upon feedback from the Authority given in the earlier investigative procedure, the prevention of abuse in connection with admission as a purpose of data processing related to admissions appeared more emphatically both in the Obligee's statements and its Privacy Rules.
Within this range, as in the case of an independent purpose of processing, the Authority regards the processing of certain personal data as acceptable based on the legitimate interest of the Controller, at the same time, only those data may be processed in such a case, which are suitable for the achievement of the purpose, thus, for instance recording a photograph and a name and the personalisation of the wristband. Recording data in addition to these, such as citizenship, type, number and expiry of the identification document, date of birth and gender fails to meet the principles of purpose limitation and necessary processing, thus the processing of these data infringed Section 4(1)-(2) of the Privacy Act.

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

In general, the Authority regards guaranteeing the safety of the visitors to the festivals as an acceptable purpose. This purpose includes both the economic interest of the undertaking organising the event and the safety of citizens, visitors as third persons from the viewpoint of data processing.

In relation to this, it is important to underline that in respect to the latter interests – provided that what we have here is an interest related to the prevention of an eventual terrorist threat or criminal acts in line with the statements of the Obligee – the Obligee essentially indicates a public interest whose enforcement, including the determination of what the public duty is and what the instruments of discharging such a public duty are, is not the Obligee's task directly, accordingly it has neither the instruments, nor the authorisation by legal regulation for the actual use of the data necessary for discharging such a duty for this purpose. Accordingly, it is not possible to refer to interests in relation to the processing of personal data, in connection to which the Controller may not lawfully take action, i.e. the processing of the data can be regarded as actually without purpose from the viewpoint of the Controller as the Controller itself cannot use the data for the enforcement of the given interest.

Deciding what threats threaten the safety of the data subject and what methods (even inclusive of data processing) can be used to efficiently combat such threats is a complex issue where the possibility to apply the law for this purpose and the suitability and necessity of the instrument to be used in this case is a means concomitant with the processing of the data which needs to be weighed simultaneously.

According to the position taken by the Authority, data processing by Sziget Kft. in connection with admissions failed to meet the conditions stipulated by the Privacy Act with respect to the latter three aspects.

In the course of examining the indispensability (necessity) and appropriateness of the practice applied, the Authority reviewed the admission practices of several European festivals of similar sizes as quasi examples of how to ensure high level protection with other methods applying instruments through which the right of the data subjects to informational self-determination is less infringed in its notice of NAIH/2017/3208/V.

In its statement dated 19 July 2017, the Obligee failed to sufficiently substantiate why other methods could not be applied in the course of admissions. The statement contained only that the solutions presented "*could not be automatically applied*" at its events, because the tickets for the festivals of the company were transferable (hence the person buying the ticket and the visitor were not necessarily identical), which "*had reasons stemming from market realities*".

The Obligee failed to substantiate the factors constituting impediments to adopting such methods in the statement referred to, as it did not throw light on "*reasons stemming from market realities*" for the Authority and also failed to justify why, for instance, the transferability of the ticket could not be limited to an earlier date, and perform personalisation in some other way that would infringe upon the data subjects right to self-determination less.

In the course of examining the issue of the suitability of the system, the Authority concluded that the efficiency of the system applied was questionable as the database was continuously being built up in the course of the personalisation of the wristbands; therefore, partly as the Obligee did not have a "reference database", i.e. it was not possible to compare the recorded data with anything and partly because the data subject was entered into the database only when he arrived at the admission gate and their ID card was scanned, the applied method puts the successful prevention of acts potentially to be committed by the data subject into question, if in the given case hours pass between being entered into the database (a few minutes after which the data subject was already in the area of the festival), and the competent organs realising a threat so as to take action against it. Let alone the

possibility of a perpetrator entering the festival area with some kind of forged document, which the Obligee was unable to filter out.

For these reasons, the Authority does not regard the instrument and method chosen to ensure the safety of visitors indispensable and suitable for achieving the desired purpose, and according to the position taken by the Authority, the scanning of the identification document and the concomitant data processing could not be regarded as proportionate to the restriction of rights caused. The absence of the suitability of data processing as the method applied also means that the processing had no genuine, lawfully acceptable purpose.

The Authority does not regard consent to the data processing carried out in the course of admissions as an appropriate legal basis, furthermore the Obligee failed to refer to legitimate interest as a legal basis, hence the Authority establishes that data processing had no appropriate legal basis during the period under study and the data processing failed to comply with the requirements of Sections 5 and 6 of the Privacy Act concerning the existence of an appropriate legal basis.

III.1.2. The period of keeping the data

The Authority establishes that in compliance with notice NAIH/2017/3208/V., the Obligee largely appropriately amended its Privacy Rules during the period under study, yet the rules contained a few deficiencies, owing to which it still failed to provide information compliant with Section 20(2) of the Privacy Act to the data subjects, even with respect to the data, whose processing was not ab ovo without a legal basis.

Thus, the Authority does not regard the period of data processing appropriate in the cases, when the Obligee retained the personal data of the data subjects beyond 72 hours following the closure of the festival for a year.

In view of the fact that the purpose of processing the data recorded in the course of admissions for more than 72 hours following the closure of the event was initiation of some kind of procedure according to the statement of the Obligee, though according to the viewpoint of the Authority, the storage of the data had no purpose after launching the procedure and the transfer of the necessary data to the Authority taking action; following the notification of the authorities this qualified as mass data processing in violation of Section 4(2) of the Privacy Act.

III.1.3. Information concerning data processing

Beyond the establishment of the infringement of legal regulations concerning the processing of the data, the Authority regarded the fact that Sziget Kft. failed to provide information on the data processors used and their responsibilities as a major deficiency. The infringement was particularly serious in the case where Netpositive Kft. played a substantial role in the process of processing the data.

In view of all this, the Authority established that during the period under study the Obligee failed to provide appropriate information to the data subjects, thus its processing of the data did not comply with the requirements set forth in Section 20 of the Privacy Act.

III.2. Data processing carried out from 25 May 2018

Under point III.2.1., the Authority separately examined the lawfulness of the processing of the data, which the Obligee processed in the course of the personalisation of the wristbands and each admission (by displaying them on the admission monitors) with a view to avoiding abuses and to protect the personal safety of the visitors. Furthermore, under point III.2.2. it separately examined the

lawfulness of the processing of the data, which the Obligee processed without displaying them on screen on every occasion in the course of admissions, but stored in a server and “used” in “exceptional” cases.

III.2.1. Processing personal data for the purpose of avoiding abuses and to guarantee the personal safety of the visitors

The Obligee produced a legitimate **interest assessment** to verify that the visitors’ interests in personal safety, the Obligee’s interests in the safe organisation of the event and the economic interests of the Obligee in preventing abuses enjoy priority against a restriction of the visitors’ right to the protection of personal data.

According to the rules of GDPR, a reference to legitimate interests as legal basis is appropriate, if the data processing serves the interest of the controller or a third person, who is other than the controller and the data subject, thus the legitimate interest of the controller or the third person is to be displayed on one side of the scales, while the legitimate interest of the data subject(s) need to be displayed on the other side of the scales in the legitimate interests assessment test, and having contrasted the opposite interest, it has to be established whether the restriction of the rights of the data subject are proportionate to the legitimate interests of the controller or the third person enforced through this restriction.

By way of an introduction to the issues related to the legitimate interest assessment, the Authority declares that it is not acceptable that the Obligee only noted in the course of examining the interests of the visitors (i.e. those of the data subject) that “the data subjects (...) objections to the processing of the data were in general as in the case of any data processing. They did not wish to have their personal data stored and processed”, i.e. the Obligee failed to examine in detail and in concrete terms what rights of the data subject were restricted by the processing, what was the extent of the restriction and whether it was concomitant with any risks; and if so, what risks were posed to the data subjects, which means that the Obligee failed to assess the opposing interests and the legitimacy of the restriction in the test. The Obligee also failed to put forward any argument of merit in its statements made in the course of the current procedure, on the basis of which it would be possible to evaluate why the interests stated by it would take precedence over the interests of the data subjects, why would the restriction of the privacy of the individual data subjects be proportionate vis-a-vis the interests of the Obligee or third persons.

The statements and documents including the legitimate interest assessment sent by the Obligee failed to verify that the data processing applied would be suitable for the achievement of all of the data processing purposes described in the test, i.e. that the processing of the data could be lawful as detailed under points III.2.1.1. and III.2.1.2.

III.2.1.1. Data processing carried out with a view to preventing abuses

It is regarded acceptable practice by the Authority if, with a view to avoiding abuses, the Obligee checks that only those persons enter the festival area to whom wristbands were assigned in the course of the first admission following the redemption of the ticket.

The Authority also agrees that the Obligee has a legitimate economic interest in preventing that more persons should enter with the tickets sold by it or scalpers on-selling tickets at a multiple price and in being able to identify stolen festival tickets in the case of theft.

According to the position taken by the Authority, the legitimate interest of the Obligee in avoiding abuse qualifies as a substantial economic interest of the Obligee, which in a given case could enjoy priority over the visitors’ right to the protection of their personal data, hence the restriction is not

necessarily disproportionate, if the Obligee handles only those personal data of the visitors, which serve the avoidance of abuses, and are necessary for the achievement of this goal, and furthermore which are suitable for the achievement of the purpose. The lawfulness of the legitimate interest as a legal basis – as a reference – definitely requires the appropriate identification of competing interests and their assessment as described above.

a) Evaluation of the suitability of data processing

As a first step, the Authority examined whether the data processing carried out by the Obligee was generally suitable for the achievement of the purposes indicated by it, whether the processing of the data could have any impact on the activities of scalpers described above, on the identification of stolen wristbands, and on preventing several persons entering the area of the festival using a single purchases and redeemed wristband.

In the Authority's view, the data processing under study is suitable for curbing only those activities of the scalpers, in the course of which they purchase tickets in advance, redeem the wristband, and resell the already redeemed wristband at a higher price. According to the Authority, however, scalpers do not sell on the already redeemed wristbands in the majority of cases, but they purchase several tickets in advance (as there is no limit on the number of tickets a person may buy) and they sell the tickets bought in advance typically via the Internet at a higher price without taking the trouble of going to the venue of the festival and exchanging them for the wristbands in order to sell the already redeemed wristbands at the venue.

In view of the fact that the personalisation of the tickets takes place in the course of the first admission when the ticket is exchanged for the wristband and not at the time of the purchase of the tickets, according to the position taken by the Authority data processing is not suitable for curbing the activities of scalpers as described above. As tickets bought in advance are not registered but they are bearer tickets, it may occur irrespective of the admission practice applied by the Obligee that a person purchases several tickets in advance, which he sells at a higher price as the person who presents the ticket at the admission gate is authorised to enter the area of the festival and not the person who originally bought the ticket.

Furthermore, according to the position taken by the Authority, data processing is not suitable for curbing the theft of wristbands from the cash desk, as the admission personnel will establish whether or not a wristband is stolen on the basis of who wishes to enter with it, i.e. for this purpose the personal data of the visitors are irrelevant, only the data identifying the wristband are relevant, on the basis of which the Obligee can establish whether or not a given wristband has been sold.

According to the view of the Authority, the practice applied earlier by the Obligee of recording the serial number of the wristbands (i.e. which wristband was issued at which cash desk and at what time) would be appropriate and sufficient for this purpose because in possession of these data it can be established whether a wristband has been stolen, saying that if there was a theft from a cash desk, then the unissued wristbands became the victims of theft.

In view of all this, the data processing carried out by the Obligee is suitable exclusively for preventing several persons entering the festival area with a single wristband, thus the only sustainable and acceptable purpose of processing the data is to filter out and curb abuses of this kind; in the other cases named by the Obligee, the data processing has no purpose, thus they infringe Article 5(1)(b) of GDPR.

b) The issue of the need for the processed data

In the case of evaluating the lawfulness of the practice, the Authority then proceeded to examine whether all the personal data displayed on the admission screens – the photo, name, gender and date of birth – are needed for the Obligee to establish whether the person intending to enter the area of the festival is authorised to do so, i.e. whether knowledge of all the data is necessary to filter out abuses, or whether the purpose can be achieved also with a narrower range of data held.

The Authority is unable to agree with the argument of the Obligee according to which the display of this range of data upon admission and its checking is needed because it may not be possible to identify a visitor based on the photo of the person obtained from the document or taken on the first day of the festival without any doubt, and in possession of these additional data (name, date of birth and gender), the admission personnel can ensure the identity of the person wishing to enter with checking questions in case of doubt.

According to the position taken by the Authority, what has significance with a view to filtering out abuses is not exactly who wishes to enter the area of the festival, but whether the person wishing to enter and the person assigned to the wristband are one and the same; from this point of view the person's date of birth and gender have no relevance, as the image displayed on screen and the name should suffice for the admission personnel to establish identity.

The Authority agrees with the statement of the Obligee, according to which the photo in the identification document is not always suitable for the identification of the holder of the document beyond any doubt, for instance, if the document is very old, but this identification beyond any doubt can be realised by making a photo of those visitors who cannot be unambiguously identified on the basis of the photo in their identification documents on site, thus knowledge of the date of birth and gender is not necessary.

According to the standpoint of the Authority, the argumentation of the Obligee is wrong also because the processing of the other data is not suitable for the identification of a person because anyone can memorise three items of identification data, thus if the admission personnel is unable to decide based on the photo displayed whether the person wishing to enter with the wristband presented upon admission is authorised to do so, the person able to answer the checking questions, i.e. if he can remember the gender and the date of birth of the real person authorised to enter will not help either.

Therefore, the image and name of the person wishing to enter shown in the admission screen should suffice for identification in the course of admission; if the admission personnel have any doubt about the authorisation of the person to enter when these data are displayed, they may call upon the person to present his identification document, because only this method is suitable for the identification of a visitor beyond any doubt.

In view of all this, the processing of the gender and date of birth of the visitors in addition to their photo and name on the admission screens is neither necessary, nor suitable for preventing abuses according to the viewpoint of the Authority, hence the processing does not comply with the requirements according to Article 5(1)(c) of GDPR and consequently, it cannot be regarded as lawful according to Article 6(f) of GDPR.

III.2.1.2. Data processing carried out with a view to guaranteeing the personal safety of visitors

In the course of the evaluation of the lawfulness of the practice, the Authority also examined whether all the personal data (photo, name, gender and date of birth) displayed on the admission screens in the course of the personalisation of the wristbands are necessary to enable the Obligee to prevent terrorist acts and other violent or drug-related criminal acts based on these data, and whether data processing is generally a suitable method to achieve these purposes, and if so, the range of data processed by the Obligee is suitable for this.

With respect to these issues, the Authority refers back to point III.1.1.2. b) above, primarily to the fact that the interests herein indicated by the Obligee are in fact purposes in the public interest whose enforcement is not the Obligee's responsibility. This in itself would not necessarily render the data processing by the Obligee unlawful, at the same time – as it is to be explained below – through linking its own data processing to the enforcement of purposes for which it does not have the appropriate instruments, essentially the Obligee conducts data processing without a legitimate purpose; if the enforcement of the given interest and the specification of the public duty and the instruments of discharging it are not directly its responsibility, then it does not have the appropriate authorisation for the data processing needed for this, for actually using the data for such a purpose. Article 6(1)(f) of the General Data Protection Regulation does not provide a basis for processing data with reference to interests, in relation to which the controller cannot lawfully take action or cannot bring measures, which is to say that the processing of these data can be regarded as actually being without a purpose from the viewpoint of the controller.

All this does not mean the questioning of the legitimacy of the purposes indicated, nor that security considerations could not arise in the course of the processing of genuinely necessary specific data with a view to a legitimate purpose that can be genuinely achieved and enforced by the controller (such as the protection of the health of the persons at an event), but these may make the enforcement of interests other than those in the public interest indicated by the Obligee and other data processing necessary, which would be evaluated very differently.

Although the Authority acknowledges the economic interest of the Obligee in organising secure events, but in its view the purposes indicated by the Obligee (prevention of terrorist acts, violent and other, drug-related criminal acts) can be implemented only through cooperation with the organs authorised thereto, the Obligee itself may not step into the shoes of the authorised public actors.

The Authority also refers to the fact that the duties of the competent public organs, the discharge of these duties and the related data processing are governed by legal regulation. With regard to the discharge of the public duties at issue, the legislator did not impose tasks for the organisers of the events; to date, the legislator has not enacted any legal regulation, which would render the processing of data mandatory at major musical or dance events presumably at higher risk with a view to combating the terrorist threat, i.e. the legislator wished to resolve the issue of terrorist threats via means other than data processing under study.

The Authority continues to maintain its position expounded in the notice sent in the course of the earlier investigative procedure and it deems that the purposes indicated by the Obligee cannot be primarily achieved through processing personal data by the Obligee, but using other means, such as physical screening, metal detectors, adequate security personnel and cooperation with the police and other agencies.

Naturally, there is nothing in principle to impede the authorities authorised to take the necessary measures with a view to handling the security risks at issue, taking measures including the processing of data within the limits of the legal regulations applicable to them, and so they themselves may carry out data processing activities, or they may order the organiser of an event or other persons to do so within the necessary range and up to the necessary extent, but this is not the case here, as the Obligee has been carrying out this type of data processing without being obligated to do so by legal regulation or an order from the authorities.

a) Evaluation of the suitability of data processing

In view of the above framework, the Authority also examined the suitability of data processing for the achievement of the purposes set and they found that the practice earlier applied by the Obligee was

not suitable for the achievement of the purpose specified by it, because during the last three years when the admission system under study was operated, the most significant and only request by an authority of such nature was when the Obligee forwarded the birth name and date of persons already admitted to TEK once or twice a day during the period of an event from the data of the admission system. Such a solution was obviously unsuitable for prevention, because the person constituting a threat has long since been in the area of the festival when the information concerning his person was forwarded to TEK.

In its attempt to prove the lawfulness of data processing, the Obligee referred to the generally preventative nature of the admission practice, i.e. that data processing in the course of admissions is generally suitable for curbing the number of the named criminal acts.

The Obligee failed to appropriately substantiate that the application of the admission system had any impact on the reduction in the number of criminal acts, thus it did not prove that the admission system would be suitable for general prevention in any way whatsoever.

The articles in the press referred to by the Obligee – which indicate the official communications of the Budapest Police Headquarters as their source – report only on the fact that due to the work of the police, the number of criminal acts continuously declined year after year from 2016 to 2017, then from 2017 to 2018 and none of the articles write about any impact of the data processing carried out in the course of admissions on changes in the number of criminal acts.

In view of the fact that the Obligee applied an admission practice including data processing in 2016, 2017, as well as 2018 each, thus any impact of the data processing carried out in the course of admissions on the number of criminal acts committed is not proven, particularly in view of the fact that the least number of criminal acts took place at the 2018 festival, in spite of the fact that Obligee processed less data this year than in the earlier years.

As neither of the articles, nor the Budapest Police Headquarters communication compare the criminal statistics of the festivals prior to and after the application of the admission system, it cannot be established that the number of criminal acts declined due to the admission system, i.e. the Obligee failed to appropriately verify that the processing of the data would be suitable for the achievement of the indicated purpose of processing, that is, the prevention of terrorist and other criminal acts.

In view of the fact that the Obligee does not apply any algorithm, on the basis of which it could establish which person could be a potential perpetrator of a given criminal act, and that it has no access to any registry, i.e. at the moment of admission it has no information which person may eventually commit a criminal act, according to the position taken by the Authority, the processing of personal data is not suitable for the prevention of terrorist and other criminal acts.

According to the view of the Authority, the data processing cannot be suitable for curbing criminal acts because in the course of applying the admission system, all the Obligee learns is who is staying in the area of the festival. It cannot, however, establish who committed a criminal act in the area of the festival merely as a result of applying the admission system. Obligee can only establish the identity if the perpetrator with the help of the data processed as a result of the practice applied, if he is caught in the act and identifies him on the basis of the information obtained from his wristband, this data processing is not at all necessary because the Obligee or the competent authority may call upon the person caught in the act to verify his identity.

In view of all this, the Authority takes the view that the processing of the data would be suitable for the achievement of the purpose identified by the Obligee in a single imaginary case, namely if the competent authority gave them a list including the group of persons, who are former or potential future perpetrators, persons constituting threats, whose entry to the festival area must be prevented and the

law enforcement organs must be notified, i.e. if the Obligee had a so-called reference database; in 2018, however, the authorities did not contact the Obligee at the festivals even on a single occasion. In such a case this would be a data processing activity according to the orders of the given authority using the data processed by the given authority, where the purpose of the data processing would not be specified by the Obligee.

According to the position taken by the Authority, what has significance in preventing terrorist acts and other violent or drug-related criminal acts is not who exactly is the person who attempts to enter the area of the festival, but whether the person wishing to enter is a person who is included in the list of persons given by the authority to the Obligee, and then the birth date and gender of the person have no significance, because the photo and name displayed on screen should suffice for the admission personnel to filter out the person who is a "potential threat" and in the given case they should call upon him to verify his identity. If the visitor arrives with genuine documents, he can identify himself appropriately, and if the document he holds is forged, the data obtained from it would be fictitious, hence the processing of the data would not be suitable for the achievement of the purpose.

The data processing carried out by the Obligee in the manner studied – with regard to data over and above the name and photo of person being admitted – is of a mass processing nature based on the above and it cannot serve the specified data processing purpose, it is not suitable for the achievement of this purpose.

Pursuant to the principle of accountability, the controller is responsible for proving that the data processing applied by it complies with the principles in the regulation, hence inter alia it has to adequately prove that its data processing complies with the principles of purpose limitation and data minimisation, which the Obligee failed to do.

In view of all this, the Authority *established that the processing of personal data was affected without a specified lawful purpose during the period under study, thus it failed to comply with the requirements set forth in Article 5(1)(b) of GDPR.*

As the data processing applied by the Obligee is in general unsuitable for the achievement of the purposes it indicated, and furthermore the Obligee failed to substantiate the conditions of applying legitimate interest as the legal basis in its legitimate interests assessment test, it failed altogether to identify the interests of the data subjects, andso it did not actually carry out a genuine assessment, the data processing fails to comply with the requirements set forth in Article 6 of the regulation.

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

Reading from the identification document, but without copying it, the Obligee records the first name and surname, date of birth, country of origin, nationality and gender of the data subject, as well as the photo in the document, or if the recording of the photo in the document is not possible for technical reasons it takes a photo of the data subject on site.

The Authority agrees with the practice of the Obligee according to which the country of origin and the nationality of the person wishing to enter are not displayed upon admission, because these data are neither necessary, nor suitable for the achievement of the purposes indicated by the Obligee.

a) According to the position taken by the Authority, recording the country of origin – or rather the authority issuing the given document – to know which country's representative bodies have to be notified in the event of an eventual terrorist act or other criminal act is inappropriate.

This data processing qualifies as stockpiling as the specified purpose is an uncertain contingent event, an exceptional situation, which in the vast majority of cases never takes place, hence the processing

of the data on the country of origin of every single visitor for this purpose fails to meet the principles of purpose limitation and data minimisation and according to the position taken by the Authority, it breaches Article 5(1)(b) and (c) of the Regulation.

b) In the opinion of the Authority, recording the data on the nationality of a visitor is an inappropriate practice, if its only purpose is to know in what language that data subject can be communicated with in the event that the visitor loses consciousness and comes to thereafter, or is in a shock because of a terrorist action or other act.

According to the position taken by the Authority, it is not necessary to process the data on nationality for the achievement of the indicated purpose because it is an exceptional situation, which never takes place in the vast majority of cases, hence the storage of the data concerning the nationality of every single visitor qualifies as mass data processing. The Authority also assumes that foreign visitors of the festival have at least a minimal command of a widely used foreign language, in which language they may not beable to communicate fluently but can at least state their nationality and the language they understand.

The Authority considers that the data processing would not be suitable for the achievement of such a purpose in every case, because it may happen that the visitor in an "emergency" is of a nationality for whose language the Obligee does not have an interpreter, in which case the Obligee or somebody else, for instance, the Authority taking action in the given case will presumably attempt to communicate in another language to react quickly and will not look for interpreters of the mother tongue of the data subject.

The general suitability of this data processing is questioned also by the fact that there are several official languages in some countries (such as Switzerland or Belgium), hence the data of a Swiss or Belgian visitor concerning his nationality or citizenship is not suitable for establishing his mother tongue.

c) According to the Authority, the practice of the Obligee according to which it records the data of the visitors concerning their gender fails to meet the principle of data minimisation because beside the name and the photo it is irrelevant from the viewpoint of identification whether the person wishing to enter is male or female, all that has significance for identification is whether the person wishing to enter is the same person who was assigned to the wristband upon the redemption of the ticket.

In view of all this, the processing of the visitors' data on gender fails to meet the principles of purpose limitation and data minimisation, hence the data processing breaches Article 5(1)(b) and (c) of the Regulation.

As the visitors' data on their country of origin, nationality and gender are not necessary for the achievement of the purposes indicated by the Obligee and the data processing is not suitable for achieving these purposes, according to the position taken by the Authority the conditions of applying legitimate interest as the legal basis do not obtain, hence the Obligee processes the visitors' data on their country of origin, nationality and gender without an appropriate legal basis in the course of storing these personal data, hence processing these data fails to meet the requirements set forth in Article 6 of the Regulation.

III.3 The sanction applied and its justification:

III.3.1. Data processing carried out prior to 25 May 2018

In the course of the clarification of the facts of the case, the Authority established that the data processing by the Obligee related to admissions to events organised in the period from June 2016

until 24 May 2018 violated Section 4(1)-(2) and Section 20 of the Privacy Act on account of the absence of an appropriate legal basis for data processing, breach of the principle of necessity and the provisions concerning prior information of the data subjects, and the Obligee failed to comply with the requirements set forth in Sections 5 and 6 of the Privacy Act.

In view of the fact that the earlier data processing practice of the Obligee constituted an infringement, but the data processing has actually been closed, and the fact that beyond the establishment of the infringing nature of the earlier data processing, an application of a fine would have no preventive effect of merit (also in view of the changes in the legal environment in the meantime), it could only be imposed as repression and also in view of the fact that a substantial period passed since the dates of the events affected by this data processing, the Authority waives the imposition of a fine as a sanction for the unlawful data processing by Sziget Kft. during this period.

As to the question whether the Authority is entitled to impose a data protection fine, it had taken into account the rules of the SME Act: when examining whether the conditions according to Section 12/A of the SME Act apply, the Authority clarified whether the Obligee qualifies as a small and medium-sized enterprise (hereinafter: SME).

Pursuant to Section 3(1) of the SME Act, an undertaking qualifies as an SME whose total number of employees is less than 250 and its annual net sales stated in a forint amount is equivalent to 50 million euros at most, or whose balance sheet total stated in a forint amount is equivalent to 43 million euros at most.

According to the 2017 annual report of the Obligee, the average headcount of its employees was 104 and its sales revenues amounted to 1,253,917,000 forints, so it qualifies as an SME under the SME Act.

On that basis, the Authority would not have been entitled to impose a fine on account of the unlawful data processing implemented prior to 25 May 2018.

III.3.2. Data processing carried out from 25 May 2018

As specified under point III.2, the Authority established that the Obligee breached Article 5(1)(b) and (c), as well as (2) of the Regulation and its Article 6 by its data processing conducted from 25 May 2018. With respect to this infringement, the Authority regarded the imposition of a fine as a sanction as appropriate as follows.

As to the question whether or not the imposition of a data protection fine is warranted, the Authority ex officio considered all the circumstances of the case based on Article 83(2) of the General Data Protection Regulation, and Section 75/A of the Privacy Act and established that in the case of the infringement exposed in the course of the current procedure, the warning would be neither proportionate, nor having a restraining force, hence a fine has to be imposed.

In view of the fact that GDPR does not contain provisions allowing for derogation from the rules on fines for SMEs, the Authority did not take the provisions of the SME Act into account when imposing the fine.

As to whether or not the imposition of a data protection fine is warranted, the Authority considered all the circumstances of the case pursuant to Article 83(2) of GDRP. The Authority regards the imposition of the fine as necessary as the Obligee processed the personal data of hundreds of thousands of

visitors without an appropriate legal basis, infringing the principles of purpose limitation and data minimisation.

In view of this, the Authority decided as presented in the operative clause based on Section 61(1)(a) of the Privacy Act and in its current decision obligated the Obligee to pay a data protection fine.

The Authority determined the amount of the fine within its discretion based on legal regulation.

Based on the nature of the infringement – absence of an appropriate legal basis, breach of the principles – the top limit of the imposable fine is EUR 20,000,000 or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is the higher according to Article 83(5)(a) of GDPR.

When imposing the fine, the Authority took the following factors into account as aggravating circumstances:

- the number of data subjects as over eight hundred thousand people participated in the VOLT, Balaton Sound and Sziget Festivals organised by the Obligee in 2018;
- the deliberate nature of the infringement as the Obligee indicated the prevention of terrorist acts and other violent and drug-related criminal acts in its LIA test, despite the fact that in the course of the earlier investigative procedure, the Authority expressed that it did not regard data processing as a suitable instrument for the achievement of these purposes on several occasions;
- the Obligee is a dominant actor in the market of festivals and mass entertaining events, the evaluation of its behaviour is subject to outstanding public attention and may serve as an example for the other actors in the market;
- the imposed fine is able to achieve its objective, if its amount is of a perceptible extent relative to the sales revenues of the Obligee.

As mitigating circumstances, the Authority took into account that the Obligee partially complied with the earlier notice of the Authority as it no longer processes personal data on the basis of consent and it no longer scans all the data of the identification document, but takes a narrower range of data from the document.

The Obligee cooperated with the Authority in the course of the Authority's procedure and regularly responded to the communications of the Authority by the due date; however, this behaviour was not evaluated as a mitigating circumstance by the Authority as it did not go beyond meeting legal obligations.

In view of the above and the fact that the Obligee's sales revenue was 1,253,917,000 forints according to its 2017 annual report, the data protection fine imposed is of a perceptible extent, but it does not exceed the maximum of the imposable fine.

Pursuant to Section 61(2)(a) of the Privacy Act, the Authority orders the publication of its decision, including the identification data of the Obligee because the decision affects a large range of people.

IV. Other issues

Pursuant to Section 60(1) of the Privacy Act, to ensure that the right to the protection of personal data is enforced, the Authority may commence an administrative procedure for data protection ex officio. The rules of Act CL of 2016 on General Administrative Procedures (hereinafter: Administrative

Procedures Act) shall be applied to the data protection procedure of the Authority with the additional points specified in the Privacy Act.

Pursuant to Section 103(1) of the General Administrative Procedures Act, the provisions of this act concerning procedures initiated upon request shall be applied to ex officio procedures with the differences set forth in Sections 103-105 of the Administrative Procedures Act.

Pursuant to Section 38(2) and (2a) of the Privacy Act, the Authority shall be responsible for monitoring and promoting the enforcement of rights to the protection of personal data and access to data of public interest and data accessible on public interest grounds. For natural persons and legal entities under the jurisdiction of Hungary, the tasks and powers specified in the General Data Protection Regulation for the supervisory authority shall be exercised by the Authority according to the provisions of the General Data Protection Regulation and the Privacy Act. The competency of the Authority extends to the entire territory of the country.

Pursuant to Section 61(2) of the Privacy Act, the Authority may order the publication of its decision, so as to include the identification data of the controller or processor as well, if the decision concerns a wide range of persons and the gravity of the infringement justifies publication.

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

Otherwise Sections 80 and 81 of the Administrative Procedures Act shall apply to the decision.

Pursuant to Sections 112, Section 116(1) and Section 114(1) of the Administrative Procedures Act, a legal remedy against the decision is available by way of action brought before an administrative court.

The rules of actions brought before an administrative court are specified by Act I of 2017 on Procedures of the Administrative Court (hereinafter: Administrative Court Procedures Act). Pursuant to Section 12(2)(a) of the Administrative Court Procedures Act, an action against the decision of the Authority shall fall within the competence of a tribunal and pursuant to Section 13(11) of this act, the Budapest Tribunal has exclusive jurisdiction with regard to such actions.

Pursuant to Section 72 of Act CXXX of 2016 on Civil Procedures (hereinafter: Civil Procedures Act), which is to be applied pursuant to Section 26(1) of the Administrative Court Procedures Act, legal representation is mandatory in any litigation within the competence of a tribunal. Pursuant to Section 39(6) of the Administrative Court Procedures Act, unless otherwise provided by law, the submission of the statement of claim shall have no delaying effect on the entry into force of the administrative act.

Pursuant to Section 29(1) of the Administrative Court Procedures Act and Section 9(1)(b) of Act CCXII of 2015 on the General Rules for Electronic Administrative and Trust Services (hereinafter: E-administration Act) to be applied according to Section 604 of the Civil Procedures Act, the legal representative of the client is obligated to maintain contact electronically.

Section 39(1) of the Administrative Court Procedures Act specifies the date and place of submitting the statement of claim. The information on the possibility of requesting a hearing is based on Section 77(1)-(2) of the Administrative Court Procedures Act. Section 44/A(1) of Act XCIII of 1990 on Levies (hereinafter: Levies Act) specifies the rate of the levy on procedures in front of an administrative court.

Section 59(1) and Section 62(1)(h) of the Levies Act exempts the party initiating the procedure from paying the levy in advance.

Pursuant Section 135 on the General Administrative Procedures Act, the Obligee shall pay a penalty for delay whose rate corresponds to the lawful interest rate if the Obligee fails to meet its payment obligation when due.

Pursuant to Section 6:48(1) of Act V of 2013 on the Civil Code, in the event of a debt that the Obligee has to pay a penalty for delay whose rate is equivalent to the base rate of the central bank in force on the first day of the calendar half-year affected by the delay as from the date of falling into delay.

Budapest, 23 May 2019

Dr. Attila Péterfalvi
President
Honorary university professor

DELIVERY CLAUSE			
To be received by:			
	Name, mailing address of the Recipient:	**To be enclosed:**	**Mode of mailing**
1.	Dr. Miklós Vida attorney-at-law Budapest Zugligeti út 41. 1121	-	acknowledgement of receipt
2.	Archives	-	-
4.	Fine register	-	Electronic copy

Publication clause to document NAIH/2019/55/5.

1. Date of publication:	
immediately	
after delivery	X
x not to be published	
2. Form of publication:	
in full	X
abridged version	
communique	
3. Data content of the publication:	
anonymised	X
anonymised, but with data of public interest accessible	
full data content	
subject matter of the case	Data processing by event organisation