Is It Really Necessary: GDPR Case Study of Sziget Music Festival Check-In

Yanzhi Xin
Brown University

Abstract

The Hungarian National Authority for Data Protection and Freedom of Information (NAIH) issued its highest data protection fine (€92,146, consisting 2.3% of the company's net revenue) to Sziget, one of Hungary's largest multicultural music and arts festivals on May 23, 2019. The organizer of this festival was found to have violated Art.5(1)b), Article.6, and Article.13 [1] of the GDPR. The violation concerned the security screenings of festival attendees by photocopying ID cards and taking photos upon entrance.

1 Introduction

Terrorist attacks in Paris in 2015 have caused major events organizers to be more cautious about their check-in systems. The organizer of Sziget music festival updated their system in response to the terrorist threat.

From June 2016 to May 24, 2018, and subsequent to the events of May 25, 2018[2], the NAIH found violations of law during the check-in process of Sziget Music Festival. In this period, the system would photocopy attendees' ID cards and take photos of attendees while not adequately informing them about why they had to collect this information, what it was going to be used for, and the duration of storing copies of their ID cards. The attendee's consent was not voluntary because they would have been denied entry if they had not agreed.

In 2016, the NAIH received complaints regarding the aforementioned admittance practice. After investigations, there were violations of GDPR found during the admittance process and the NAIH imposed its highest fine of €92,146 against the organizer of Sziget and called on the organizer to review and modify its check-in system and data processing practices, and to align with GDPR rules in the course of admittance.

The case was concluded on May 25, 2018 and the organizer of Sziget paid for 3 million HUF fine (approximately €92,146) within 30 days from the date when the order was issued.

2 Background

The Hungarian Parliament have carried out several GDPR implementation packages to bring Hungarian law to align with the GDPR as Hungary being a member of the EU. The current main national law on personal data protection is Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (the Act) to implement the GDPR[3].

With the effect of 26 July 2018, the Hungarian Parliament has amended the Act to comply with the GDPR. The Authority also stated that the GDPR shall prevail if there is any direct conflict between it and the Hungarian privacy rules.

The GDPR implementation in Hungary applies to all kinds of data processing operations, except to the processing of personal data by a natural person in the course of a purely personal or household activity. This implementation also covers manual data processing operations as an addition to the GDPR.

On 26 April 2019, the Hungarian Parliament has further amended the Act[3] — At the request of the National Authority for Data Protection and Freedom

of Information (NAIH), a local government notary is required to verify the actual circumstances of the data processing activities of a data controller including the scope of the personal data processed, the means of the operations, and the technical and organizational measures.

3 Relevant Roles

3.1 Data Subject

Attendees of the Sziget Music Festival from June 2016.

3.2 Data Controller

Data collection during check-in process of the festical was carried out by Sziget Kulturális Menedzser Iroda Kft (Sziget Kft.). They scanned attendees' ID cards and read, recorded and stored the following data of the data subjects: citizenship, name, gender and date of birth. In addition, videos and sound recordings of attendees were also stored and processed by Sziget Kft.

3.3 Data Processor

Sziget Kft. was responsible for data processing after they gathered attendees' information.

4 GDPR Violations

4.1 Article 5(1)(b)

The processing of the attendees' gender information fails to meet the principles of purpose limitation and data minimization[4]. Their personal data also should not be further processed in any manner that is incompatible with the organizer's purpose of preventing terrorist attacks.

4.2 Article 6

The processing of the gender and date of birth of attendees in addition to their photo and name on the admission screens is neither necessary, nor suitable for preventing abuses. It cannot be regarded as lawful.

4.3 Article 13

Sziget Kft. failed to provide the data subjects with adequate information regarding the purpose or the basis of processing their personal data upon entrance.

5 Response

Sziget Kft. presented that the purpose of data processing of the check-in system was designed to ensure that the persons indicated by authorities that might be involved in terrorism were filtered out and prevented from entering the event.

The system recorded attendees' photos and images of their identification document, which was stored in their own internal database on their own servers. 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"[2].

The NAIH thus thinks that the data processing in relation with the check-in is not capable to prevent crimes since it does not have a reference-database with which he could compare the data collected at the check-in, thus in reality it's not possible to filter out the possible perpetrators and the lawfulness of this action can't be established[2] .

6 Prevention

6.1 Human Factors

The check-in system for this music festival was designed to safeguard festival-goers' personal security but ended up infringing on their privacy. The organizer should have given clarification on the purposes of data processing and how long their information was going to be stored.

On the other hand, the Data Protection Authority (DPA) (the NAIH in this case) should have provided guidelines on the data processing for mass events. The organizers would have known the limitations and restrictions enforced by the GDPR and aligned with such rules.

6.2 Data Processing and Storage

The organizer could have prevented this by following data minimization and storage limitation rules[4]. For data minimization, it really wasn't necessary to store information like date of birth, gender, age, nationality, and the attendee's photo upon entrance. For data storage, the organizer should have erased all of the attendees' data including videos and audio recordings after the screening was over.

In addition, security screening could have been achieved without any data processing or storage by installing metal detectors or other security devices at festival venues[5].

References

[1] GDPR Enforcement Tracker, https://www.enforcementtracker.com

[2] Sziget Final Decision, https://tinyurl.com/y3enyxcj

[3] Hungary - National GDPR Implementation Overview, https://www.dataguidance.com/notes/hungary-national-gdpr-implementation-overview

[4] Data Protection in Hungary https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2020/hungary

[5] Sziget Festival Fined Record HUF 30 Million for GDPR Breaches – What Went Wrong? https://tinyurl.com/y47zz26h