04 June 2020

Final Decision

Complaints against [redacted] – Lawfulness of the processing (Article 6 GDPR)

IMI A56ID: 81381
IMI Case: 92167
IMI A60DD: 92290
IMI A60RD: 125912

The Hessian Commissioner for Data Protection and Freedom of Information (hereinafter "HBDI") refers to various complaints against [redacted] (hereinafter "[redacted]) concerning [redacted]s authentication and identification procedure.

1. Case Description

HBDI has received several complaints against [redacted] regarding its authentication and identification procedure when confronted with claims for compensation payments by [redacted]. To ensure the compensation payments reach the entitled recipient, [redacted] had asked the claimants for proof of identification and required "a selfie photo of the [redacted] holding their valid government issued ID (e.g. passport, ID card, driver's license) with their face clearly visible". The complainants considered this identification procedure unlawful.

2. Investigation Procedure

HBDI contacted [redacted] in July 2019. In its answer, [redacted] stated that under the current [redacted] the company is obliged to pay compensation to [redacted]. [redacted] added that failure to comply with other parts of the contract, such as the [redacted], might also result in compensation under the [redacted]. However, it must always be ensured that the demanding person is an entitled [redacted]

In this respect, [redacted] was able to demonstrate to the HBDI that the identification of a person entitled to claim is not sufficient solely based on the booking data [redacted], since [redacted] are often disposed of or not securely stored by [redacted] after the [redacted] This means that third parties can easily access

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

the relevant data. Furthermore, information about a [redacted] is accessible to everyone via publicly accessible platforms (such as [redacted], etc.). Consequently, a third party who obtains the booking data, for example by finding a lost [redacted], can very quickly find out whether she or he can assert illegitimate claims for [redacted]. The same also applies to [redacted], as only the knowledge that the [redacted] has been [redacted] is required.

Furthermore, [redacted] explained that due to a significant increase in fraud incidents and in order to protect actual claimants, measures were introduced which should contribute to the unambiguous identification of the claimant. As a result, in addition to the booking data [redacted]) and the [redacted]'s name, [redacted] also requested a copy of the claimant's ID and a photo showing the claimant together with his ID.

[redacted] stated, however, that the request to send a photo and a copy of the ID should only be made if the claimant could not be unambiguously identified otherwise. As soon as the e-mail address, telephone number or (for letters) the address was identical with the contact data from the [redacted] or the [redacted] profile, the claimant was deemed identified.

In this context, [redacted] was able to demonstrate to the HBDI that it is often not possible to unambiguously identify the claimant on the basis of the data available to the company.

[redacted] explained, for example, that if a [redacted] books his or her [redacted] through a [redacted], [redacted] does not have the [redacted]'s contact details because they are either not entered by the [redacted] or the [redacted] passes on its own contact details.

Identification by comparing the [redacted] information is also not possible, since the [redacted] data is processed in a completely separate system and customer complaint management is not given access for reasons of data minimization. Moreover, the data were not useful for identification purposes.

[redacted] further stated that a comparison with the [redacted] data is only possible if the [redacted] number had already been entered at the time of booking. However, this is not necessary.

[redacted] also explained that the exclusive transmission of a copy of the claimant's ID does not seem to be a viable alternative either, given the high number of cases of fraud in which manipulated IDs were submitted. Since [redacted] serves customers all over the world, [redacted] would have to know the security features of the ID cards of all countries in order to be able to detect manipulations.

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

In the course of the proceedings, [redacted] was thus able to demonstrate to the HBDI that a clear identification of the demanding person is required in the event of reimbursement proceedings on the company's part.

On 30 October 2019, HBDI met with [redacted]'s DPO to discuss the proceedings. During this meeting, [redacted] stated that due to the increasing uncertainty of [redacted]'s customers, it had already stopped requesting a photo of the persons concerned since 1 October 2019 to ensure identification in the context of processing reimbursement transactions. On the same day, [redacted] also acknowledged in writing that the identification procedure in question had already stopped.

In this context, HBDI and [redacted] agreed that in order to counter possible fraud in future, [redacted] may consider other less intervention-intensive identification procedures but inform the HBDI prior to their introduction.

In its Draft Decision of 21 November 2019 (IMI A60DD 92290), HBDI concluded that since [redacted] had stopped the identification and authentication procedure in question, the complaints have been settled and the proceedings can be concluded.

The Portuguese, Finnish and Belgian Data Protection Authorities commented on the HBDI's Draft Decision:

The Portuguese Data Protection Authority raised an objection stating that the decision covers several complaints but does not specify for each of them whether there has been effective collection of data on the identification and authentication procedure. Further, the Portuguese DPA noted that the HBDI's Draft Decision does not mention whether data have been erased, since the identification mechanism has already been suspended.

The Belgian and the Finnish DPA also commented on the Draft Decision and stated that requiring "a selfie photo of the [redacted] holding their valid government issued ID (e.g. passport, ID card, driver's license) with their face clearly visible" was in contradiction with the data minimization principle (Article 5(1) lit. c GDPR). Besides, the Belgian DPA wondered whether or not an [redacted] active worldwide and especially in the European Economic Area, should not be in a position to have some knowledge of the security features of the European official IDs and that when the [redacted] has been booked by an intermediary such as a [redacted], it does not see why [redacted] would not be in a position to reach the [redacted] and cross-check the data it got from the consumer claiming some compensation (reimbursement), especially for instance, beyond the contact details of the consumer, his/her bank account number.

In its Revised Draft Decision of 18 May 2020 (A60RD 125912), HBDI replied the following in response to the objections from Portugal: The complaints received by the HBDI concerning [redacted]s authentication and identification procedure have been dealt with individually and the complainants have received individual answers to their specific complaints. The HBDI chose to create only one Article 56 procedure and only

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

one entry in the Case register for these complaints as they are about the same controller, same type of complaint and same type of data processing. This is in line with the recommended practice developed by the IT User Expert Subgroup and reflected in the EDPB IMI User Guide for bundling complaints to avoid the creation of a high number of unnecessary Article 56 procedures and reduce workload for Supervisory Authorities.

Further, HBDI informed the Portuguese DPA that there has not been effective collection of personal data in the course of the identification and authentication procedure, since many complainants refused to submit a selfie and lodged a complaint with the HBDI instead. When personal data was collected, HBDI has received the confirmation of cancellation from [redacted]

In response to the comments of the Belgian and Finnish DPA the HBDI stated the following: The HBDI does not regard [redacted]s authentication process as a violation of the obligation to minimize data in accordance with Article 5(1) lit. c GDPR. [redacted] request to submit a selfie with photo identification was an immediate measure and was introduced as an interim solution until online and video identification procedures were developed, established and evaluated. It was introduced since an auditing firm commissioned by [redacted] had found that the number of suspicious refund claims in the first quarter of 2019 had amounted to 400.000,00 EUR. In the first quarter of 2015, by way of comparison, the figure was 1.423,00 EUR. In 2018 and the first quarter of 2019 there had been a significant increase, which prompted [redacted] to take investment measures. The results of the audit by the auditing company were presented to the HBDI. It was suspected by [redacted] that organised criminals had discovered a possibility for themselves to obtain unjustified payments. In view of the high losses, a quick reaction by [redacted] was necessary to avert further damage. Up to this point in time, the customer complaint management had no contact with the examination of the forgery-proofing of copies of identification documents and has to process approximately 5000 refund claims per day. In addition, genuine copies of ID cards were probably also presented without justification. A large number of [redacted] are still booked through [redacted]. These agencies are then in possession of copies of [redacted] ID cards. There is no legal obligation for [redacted] to hand over their customers' information to [redacted] The [redacted] also require a data protection legal basis for the release. On the other hand, the [redacted] are - especially with regard to account data - under no obligation to disclose customer data. Furthermore, it could not be ruled out that in some cases the [redacted]/their employees themselves might be involved in the alleged fraud. [redacted] has credibly argued that authentication based solely on the booking data [redacted]) was not sufficient to contain the above-mentioned damage. It was clear that the demand for additional authentication factors was legitimate. During this investigation procedure and until the investigated authentication procedure was discontinued, no milder measures were discernible which would be suitable to the same extent to avert the

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

financial damage. The termination of the authentication procedure on the part of [redacted] was not due to data protection reasons, but rather to customer dissatisfaction and the increasing number of complaints.

3. Decision

Since the objections and comments made against the Draft Decision were adequately addressed and there were no objections to the Revised Draft Decision by the Supervisory Authorities concerned, the proceedings can be concluded.

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de