Berlin Commissioner
for Data Protection
and Freedom of Information

521.14435.6
CR 191470
DD 469870

Berlin, 17.05.2023

Final Decision

Preliminary remarks

The complaint (ref. no. 521.14435) was raised before the Berlin DPA in April 2021. It was transferred to the supervisory authority Netherlands, which is the Lead Supervisory Authority (LSA) for the cross-border processing carried out by [redacted] in accordance with Article 56 GDPR. The LSA conducted the investigation and the cooperation procedure with all concerned supervisory authorities in accordance with Article 60 GDPR. The LSA proposed a Draft Decision and thereby the complaint was rejected. In accordance with Article 60 (8) GDPR, the Berlin DPA as the supervisory authority with which the complaint was lodged, hereby adopts the decision as it was agreed upon in the cooperation procedure and is included below:

Summary of the Case

1. On 28 June 2020 the complainant made a booking via the platform [redacted] for the accommodation [redacted] On 29 June 2020 he received a notification from this accommodation in which they invited him to contact them at [redacted] After contacting the e-mail

Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI)
Alt-Moabit 59-61, 10555 Berlin
Germany

Phone: +49 30 13889-0
Fax: +49 30 215 50 50

Office hours: Monday to Friday from 10 am to 3 pm, Thursday from 10 am to 6 pm

E-mail: mailbox@datenschutz-berlin.de
Website: www.datenschutz-berlin.de

address he received an e-mail from another e-mail address on the same day stating that [redacted] had not updated the calendar for the booked accommodation, therefore his booking was not possible. After some e-mails back and forth the complainant opted for a comparable accommodation [redacted] and paid the requested amount to a Spanish bank account. Upon arrival the complainant had found that the accommodation did not exist and that he had been the victim of fraud.

2. The complainant suspects that there has been a data breach at [redacted], given that he had been contacted with precise information about his planned stay in [redacted]

Investigation by the NL SA

3. On 19 August 2022 the NL SA requested additional information regarding this complaint from [redacted] The NL SA requested [redacted] to clarify if the complainant had contacted [redacted] about his experience with the initial accommodation provider [redacted] The NL SA also asked [redacted] has been identified by [redacted] as a fraudulent accommodation provider. On 8 September 2022 [redacted] replied to this request.

4. [redacted] replied that they found no contact between them and the complainant in relation to his concerns about the accommodation. [redacted] confirms that the accommodation provider was identified as fraudulent by [redacted] on 30 June 2020. [redacted] explains that in their standard procedures, this triggers a cancellation by [redacted] of reservations made on the platform with the accommodation provider. In relation to this specific reservation [redacted] systems show that the complainant had already cancelled the reservation himself. The cancellation was free, so the complainants credit card was not charged at that point by [redacted]. Additionally, since the payment was handled directly by [redacted], the accommodation provider would not have received any payment details relevant to the complainant from [redacted]

5. [redacted] informed the NL SA that the fraudulent accommodation provider has invited the data subject to reply via an email address shared by the fraudulent accommodation provider [redacted] states that if the complainant did respond directly to this email address and not via the [redacted]

platform, it is possible that the complainant may have provided personal data to the fraudulent accommodation provider directly, including potentially his credit card details. [redacted] clarifies that this would have taken place outside of the [redacted] platform and would therefore not be visible to [redacted]

6. The NL SA looked into the communication between the complainant and the fraudulent party, and have confirmed that the complainant emailed directly to the fraudulent party.

7. On 12 September 2022 the NL SA contacted the Berlin SA via 61VMN 436950 and shared the reply of [redacted] and an assessment of the case. The NL SA invited the Berlin SA to share the reply of [redacted] with the complainant. The NL SA believed that there was no indication of a GDPR violation and asked the Berlin SA if it was possible to contact to complainant and ask him to withdraw his complaint. On 21 November 2022 the NL SA sent a reminder to the Berlin SA via 61VMN 460002 and asked if the Berlin SA agreed with the NL SA's assessment of this complaint. The NL SA has not yet received a response from the Berlin SA.

Norm allegedly infringed

Article 32 GDPR

Proposed action by the NL SA

8. Considering the above the NL SA finds no infringement of the GDPR in this case.

9. The NL SA deems this matter investigated to the extend appropriate and rejects the complaint ex article 60(8) GDPR. The supervisory authority with which the complaint was lodged (the regulatory authority in Berlin) shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

Appeal Notice to the complainant

Against this decision a lawsuit before the Verwaltungsgericht Berlin (administrative court of Berlin), Kirchstraße 7, 10557 Berlin is admissible. The lawsuit needs to be filed in written form within one month after the notification of this decision, it can also be filed as an electronic document with a qualified electronic signature (QES) or for the record of the

clerk of the court. Please, note that in case of filing the lawsuit in writing the legal deadline is only met if the lawsuit reaches the administrative court within the deadline.

The Berlin Commissioner for Data Protection and Freedom of Information