TO THE AUTORITEIT PERSOONSGEGEVENS (AP)

HOGE NIEUWSTRAAT 8, 2514 EL THE HAGUE, NETHERLANDS

Complaint pursuant to art. 77 of Regulation (EU) 2016/679.

The undersigned, Luca Di Garbo (the "**Complainant**")…*(omissis)* … hereby declares for the purposes of this proceeding that he wishes to receive any communications at the following address: *(omissis)*, and sets out the following:

a) The complainant is a resident of the Italian Republic and has been the holder of a booking account since 2015.
b) For the purposes of this complaint, Booking.com B.V., headquartered in Amsterdam, Netherlands, is identified as the Data Controller responsible for the processing of the complainant's personal data. As the Data Controller, Booking.com B.V. bears primary responsibility under the GDPR for ensuring the security, integrity, and lawful processing of personal data.
c) The incident at the heart of this complaint originated from a legitimate and routine booking made by the Complainant through the Booking.com platform. On 5 March 2025, the Complainant successfully booked an accommodation in Naples, specifically "The Other Duomo House By House," for a stay from 28 March 2025 to 30 March 2025 (Annex 1).
d) This initial authorized transaction is a critical precursor, as it established the direct data processing relationship between the complainant and Booking.com B.V., thereby placing the subsequent handling of the Complainant's personal data squarely within Booking.com's responsibility.
e) The integrity of this data processing was demonstrably compromised on 27 March 2025, the day prior to the scheduled check-in.
f) On this date, the Complainant was contacted via WhatsApp by an individual identifying as "Elainne", purportedly the "check-in manager" of "The Other Duomo House By House" (Annex 2). The message asserted an inability to process the Complainant's bank card, claiming it was either declined or invalid, and demanded confirmation of card details or the provision of an alternative.
g) Clear and strong pressure was exerted on the Complainant failure to complete this "verification" via a provided link within 24 hours would result in the automatic cancellation of the booking. The link provided remains active as of the date of this complaint with Booking DPO (Annex 3), and upon accessing the chat box, it explicitly requests entry of card details (Annex 4).
h) Crucially, on the very same day, the Complainant received an email at the address used for the booking (Annex 5) and a corresponding message within the Booking.com internal mailbox (Annex 6). Both communications originated from "The Other Duomo House by House in Naples (via Booking.com)" and, significantly, bore the domain name @property.booking.com.
i) This domain name, combined with the precise knowledge of the Complainant's booking details – including the specific accommodation, dates of stay, and personal identifiers – lent

an overwhelming air of credibility to the fraudulent communications. The content of these email and Booking.com messages mirrored the WhatsApp message exactly, reinforcing the deceptive nature of the scam attempt.

j) The Complainant contacted the Data Controller on 16 April 2025 (Annex 7), raising concerns regarding the data breach and requesting, pursuant to Article 82 of the GDPR, full and effective compensation in the amount of € 2, 500.00 for the material and non-material damage suffered as a direct consequence of the aforementioned incident and the underlying infringement of the GDPR.

k) The Complainant received a response from the Data Protection Officer of Booking.com on 24 April 2024 (Annex 8), in which it was stated as follows: *"In regard to your privacy concerns regarding Booking.com's systems being compromised, we present you the following: We do not have conclusive evidence that the accommodation partner's account has been compromised. We've received reports from some of our accommodation partners that they have been targeted by phishing emails, which in some cases may have led to their systems being compromised. The facts you have described to us and the results from our investigation show many similarities with such a phishing incident, which means that this did not take place on Booking.com's systems. Booking.com systems have not been compromised, and as we previously mentioned above, there are not enough indicators to confirm that the accommodation partner's account has been compromised, as the malicious activity may have taken place on the accommodation partner's platform, outside of Booking.com range of detection for malicious activities. We understand your concerns regarding the potential harm you might have suffered from malware, phishing and social engineering attempts by third parties to fraudulently compromise systems and accounts of accommodation partners and their properties. Booking.com will never ask for any payment or credit card details via chat messages. Customers needing to process a (pre)payment for a reservation made on the Booking.com platform can do so directly through Booking.com's platform. Meanwhile, Booking.com continues to operate and regularly enhance its security monitoring and fraud prevention/detection measures in liaison with accommodation partners to minimize impact from malware, phishing and social engineering attempts targeting accommodation partners, their properties and their customers. We trust we informed you properly."*

l) Indeed, contrary to what has been asserted by Booking.com, the sophistication and multi-channel nature of this scam indicate a profound compromise of personal data.

m) The fact that the scam was orchestrated across multiple communication platforms (WhatsApp, email, and Booking.com's own internal messaging system), coupled with the precise knowledge of the Complainant's booking details (property name, dates of stay), and the use of a highly credible sender domain (@property.booking.com), strongly suggests that the perpetrators had direct access to the Complainant's booking information within Booking.com's systems or via a deeply compromised partner system.

n) This level of detail and coordinated multi-channel delivery elevates the incident beyond a generic phishing attempt: it is a direct consequence of a personal data breach under Booking.com's control.

o) The specific data points compromised, including the Complainant's name, email address, phone number, and precise booking details, illustrate the breadth of the breach. This is not merely a list of randomly acquired email addresses; it signifies a breach of transactional data, which is inherently sensitive as it enables highly targeted social engineering attacks. The fact that the scammer knew *which* booking to target and *when* points unequivocally to a compromise of Booking.com's core booking database or a highly integrated partner's system.

p) It is evident from the content and context of the WhatsApp message, the email, and the Booking.com internal message that personal data entered by the Complainant on Booking.com, including his name, email address, and phone number, was disclosed to

unknown third parties without authorization. This unauthorized disclosure constitutes a direct failure by Booking.com to secure the Complainant's personal data.

q) The unauthorized disclosure of the Complainant's personal data, which directly enabled the attempted scam, stems from a clear failure by Booking.com B.V., in its capacity as data controller, to comply with fundamental provisions of the GDPR.

r) The incident demonstrates a profound lapse in Booking.com's adherence to core data protection principles, specifically those related to the security and integrity of personal data.

s) **VIOLATION OF ARTICLES 5(1)(F) AND 5(2) GDPR - PRINCIPLES OF INTEGRITY, CONFIDENTIALITY, AND ACCOUNTABILITY:** Article 5(1)(f) of the GDPR mandates that personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures ("integrity and confidentiality"). Furthermore, Article 5(2) establishes the principle of accountability, stipulating that the controller is responsible for, and must be able to demonstrate compliance with, these principles.

t) Booking.com B.V. has demonstrably failed to uphold these obligations. The unauthorized disclosure of the Complainant's personal data, which directly facilitated a targeted scam attempt, is irrefutable evidence of a failure to ensure appropriate security. This breach signifies a clear lack of integrity and confidentiality in their data processing operations. The very occurrence of this incident, where sensitive booking details were accessed by an unauthorized third party to orchestrate a sophisticated and targeted scam, directly violates the principle of "integrity and confidentiality". It is not merely that a scam occurred; it is that Booking.com's system, or a system under its direct control and responsibility, was compromised, allowing the scammer to obtain the precise and necessary information to execute the fraud. This shifts the focus from a generic cybercrime to a specific and undeniable failure of Booking.com's data protection measures. Consequently, Booking.com B.V. has also failed in its accountability obligations under Article 5(2), as it has not been able to demonstrate that appropriate measures were in place to prevent such an incident.

u) This is further underscored by the Dutch Data Protection Authority's (Autoriteit Persoonsgegevens - AP) previous enforcement actions against Booking.com B.V., including a significant fine in December 2020[1] for a delayed data breach notification concerning a 2018 incident where criminals accessed customer data, including names, addresses, phone numbers, booking details, and credit card information, through a scam targeting hotels using the Booking.com system. This history indicates a persistent pattern of security vulnerabilities and inadequate response to data breaches.

v) **VIOLATION OF ARTICLE 24 GDPR - RESPONSIBILITY OF THE CONTROLLER**: Article 24 of the GDPR places a comprehensive responsibility on the data controller to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation. This obligation is proactive, requiring the controller to ensure GDPR compliance at all stages of processing and to continuously review and update these measures. The incident described herein, where personal data was compromised leading to a targeted scam, directly reflects a failure by Booking.com B.V. to meet its overarching responsibilities under Article 24. The Dutch DPA has consistently emphasized the importance of robust data

[1] Dutch SA fines Booking.com for delay in reporting data breach, https://www.edpb.europa.eu/news/national-news/2020/dutch-sa-fines-bookingcom-delay-reporting-data-breach_en

protection policy frameworks and a high level of GDPR compliance maturity for organizations, indicating that a mere reactive approach is insufficient[2]. The recurrence of similar scam attempts since at least 2018, as publicly reported, suggests that Booking.com B.V. has not adequately fulfilled its continuous obligation to review and update its security measures to address evolving risks, thereby failing to demonstrate compliance as required by Article 24.

w) **VIOLATION OF ARTICLE 32(1) GDPR - SECURITY OF PROCESSING**: Article 32(1) of the GDPR requires data controllers to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. This assessment must take into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The European Court of Justice (ECJ) has clarified that while an unauthorized disclosure by third parties does not automatically prove that implemented technical and organizational measures (TOMs) were inappropriate, the data controller bears the burden of proving that the security measures taken were indeed appropriate. The ECJ emphasizes that Article 32 requires a risk management system that minimizes, rather than eliminates, all data protection risks, and national courts must concretely assess the adequacy of TOMs by examining the risk analysis and evaluating the measures' practical effects[3]. The recurring nature of personal data leaks and subsequent scam attempts linked to the Booking.com platform since at least 2018 demonstrates a systemic and unaddressed security flaw, rather than an isolated event. Public reports, such as *"Booking.com customers targeted by hackers in WhatsApp and text scam"* from Express on 4 June 2018[4], and *"Booking.com warns of up to 900% increase in travel scams"* from the BBC on 20 June 2024[5], confirm that these vulnerabilities are not new: they are well-known to the platform. The persistence of these incidents, despite years of public awareness and media coverage, leads to the undeniable conclusion that Booking.com B.V. has not implemented appropriate and effective technical and organizational measures commensurate with the high risk associated with processing sensitive booking and financial data. If Booking.com B.V. has been aware of these vulnerabilities for years and they continue to occur, it implies a fundamental and ongoing failure to implement *appropriate* and *effective* security measures as required by Article 32(1). This suggests a lack of proactive risk assessment and mitigation, undermining any claim to maintaining *"state of the art"* security. The public knowledge and recurrence of these issues significantly amplify Booking.com's culpability. The fact that these issues are widely reported and even acknowledged by Booking.com itself means they cannot claim ignorance. This indicates a systemic flaw in their security posture and a failure to adequately protect user data despite being fully aware of the risks, adding significant weight to the claim that their measures are not *"appropriate to the risk"* as mandated by Article 32(1). The Dutch DPA has also consistently highlighted the need for organizations to have robust data protection policies and practices, including those related to data breach handling and security measures.

---

[2] Dutch data protection authority raises expectations for GDPR compliance practices, https://www.pinsentmasons.com/out-law/news/dutch-data-protection-raises-for-gdpr-compliance-practices

[3] ECJ, judgment on 14 December 2023 in case C-340/21.

[4] "Booking.com customers targeted by hackers in WhatsApp and text scam", Express, 4 June 2018, https://www.express.co.uk/travel/articles/969363/Booking-com-uk-hackers-whatsapp-text-scam

[5] "Booking.com warns of up to 900% increase in travel scams", BBC, 20 June 2024, https://www.bbc.com/news/articles/c8003dd8jzeo

x) **DAMAGES SUFFERED AND RIGHT TO COMPENSATION**: Although the issue of compensation for the damage suffered does not fall within the scope of the decision requested from this Authority, the Complainant nonetheless feels compelled to point out that the conduct described above has given rise to compensable harm. Actually, as a direct result of the personal data breach and the subsequent attempted scam, which stems from processing activities under Booking.com B.V.'s responsibility, the complainant has suffered both material and non-material damage. Pursuant to Article 82(1) ofthe GDPR, any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. The ECJ has clarified that the concept of "damage" under Article 82(1) should be broadly interpreted to fully reflect the GDPR's objectives, and that a personal data breach can result in non-material damage such as "loss of control over their personal data".

y) In this context, the judgment of the General Court in Bindl v Commission (judgment of 8 January 2025, T-354/22 – under appeal) is particularly relevant. In that case, the Court ordered the Commission to pay compensation, having found that the claimant had suffered non-material damage due to being placed "*in a position of some uncertainty as regards the processing of his personal data, in particular of his IP address*".

z) The General Court clarified that uncertainty about the processing of personal data is sufficient to justify the existence of non-material damage.

aa) Specifically, the Complainant has suffered significant non-material damage, including:

- **Emotional distress and anxiety**: the targeted nature of the scam attempt caused considerable distress and persistent anxiety regarding the security of his personal and financial information held or processed in relation to his booking.
- **Well-founded fear of data misuse**: the incident has generated a justifiable and ongoing fear that his personal data has been compromised and may be misused for fraudulent purposes or identity theft, given the apparent unauthorized access or disclosure enabling the scam attempt.
- **Loss of control over personal data**: the attempted scam demonstrates a tangible loss of control over his personal data, as it appears to have been accessed and utilized by unauthorized third parties for malicious purposes.

Furthermore, the Complainant has suffered material damage consisting of:

- **Expenditure of personal time and effort**: He was compelled to expend a considerable amount of personal time and effort in verifying the legitimacy and security of his booking with The Other Duomo House By House, investigating the nature of the scam attempt, and taking steps to mitigate potential further harm. This time represents a quantifiable loss necessitated directly by the incident linked to the processing of his data by Booking.com.

All of the above considered, the undersigned:

REQUESTS

The Data Protection Authority, after examining the complaint and finding it well-founded, to take all appropriate measures, and in particular:

1. **Issue warnings or reprimands:** address Booking.com B.V. with warnings or reprimands pursuant to Article 58(2)(a) and (b) of the GDPR, clearly highlighting the unlawfulness of the data processing practices that led to the personal data breach and the subsequent security failures. This action would formally acknowledge Booking.com B.V.'s non-compliance.
2. **Implementation of corrective measures:** order Booking.com B.V. to cease the processing of personal data in a manner that leads to such breaches and to implement robust technical and organizational measures to ensure a level of security appropriate to the risk.
3. **Facilitate compensation:** implicitly or explicitly facilitate the Complainant's right to compensation under Article 82 of the GDPR.

Rome, 03/06/2025

Signature

Luca Di Garbo

Annex 1: proof of booking on Booking.com

Annex 2: fraudulent WhatsApp messages (screenshots)

Annex 3: fraudulent Booking.com webpage

Annex 4: chat box of the fraudulent Booking.com webpage (screenshot)

Annex 5: fraudulent email

Annex 6: fraudulent message in the Booking.com mailbox (screenshot)

Annex 7: letter sent by the Complainant to Booking.com on 16 April 2025

Annex 8: response from the Data Protection Officer of Booking.com received by the Complainant on 24 April 2024