Case Study of the GDPR Violation by Booking.com B.V. for its Late Data Breach Notification

Junewoo Park
Brown University

Abstract

On February 7 2019, Booking.com B.V. (“Booking"), an online reservation platform for accommodations (“Trip Advisors") and customers, notified the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, “AP") that personal data of about 4,109 people had been compromised. An unknown third party could access personal information of customers stored in Booking’s Extranet by pretending to be a Booking employee and asking Trip Advisors their specific login details for Extranet. On December 10 2020, AP imposed a fine of €475,000 on Booking for not notifying AP of its personal data breach incident within 72 hours after having become aware of it. This report reviews the data breach incident, how the decision by AP was made, and the implications of the decision.

1 Introduction

Booking is an online reservation platform based on Netherlands where its users are individual customers and Trip Advisors. Since the customers need to provide Trip Advisors with their contact, reservation, and payment data, Booking shares the customers’ personal information with appropriate Trip Advisors via secured Extranet. Representatives to each accommodation can access shared private data of its prospective customers by filling in its username, password, and a “2FA code." [1]

In December 2018, an unknown party began calling hotels and managed to learn login details for Extranet from 40 hotels by posing as an employee of Booking. By logging in to Extranet using the phished information, the cyber-criminals were able to access to 4,109 people’s data. According to the final Security Incident Summary Report submitted to AP from Booking, personal data including name, phone number, reserved hotel nights, reservation number, and price per night were compromised. For 283 customers, their credit card data was compromised, and 97 among them even had their CVCs compromised. [1] After some investigation, AP decided to impose a fine of €475,000 on Booking. Booking did not contest.

The following section will examine how Booking came up with this decision: (1) Booking is guilty of violating GDPR; and (2) The fine should be €475,000. Then, the last section will discuss the significance of the decision of AP made on this incident.

2 GDPR Violation

2.1 The Violation

AP concluded that Article 33(1) [2] was violated by Booking:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

According to the decision document by AP [1], Booking received several emails from two Trip Advisors between January 9 and 20 2019 that their guests had received phone calls and an email asking personal information about the guests. The strangers who contacted the guests knew about their reservations and required credit card details or birth date needed to process their payment. On January 31, Booking’s Security team started investigated the matter and released a preliminary report on February 4 that confirmed the breach. Booking reported the incident to AP on February 7, which was within 72 hours after the confirmation of the breach.

Since the second email from a Trip Advisor on January 13 clearly demonstrates that someone who knew reservation details of customers contacted them for personal information,

AP concluded that Booking should have notified AP within 72 hours after that day, namely until January 16. Booking was late for 22 days according to AP, violating Article 33(1) of GDPR.

2.2 The Fine

Since 2019, AP has been applying their own policy of fining data controllers and processors who violate GDPR. [3] The policy divides possible scenarios of GDPR violation into four categories depending on their seriousness. For each category, there is a range of fine that can be imposed, with its basic fine defined as the middle point of that range. After deciding the category of an incident of violation, AP then decides whether to increase or decrease the fine starting from the basic fine considering the factors derived from Article 83(2). The refinement factor are stated in Article 7 of the fining policy [4] and include 7(a) nature, gravity, and duration of the violation, 7(b) intentional or negligent character of the violation, and 7(c) any action to reduce the damage from the violation.

The violation of Article 33(1) is classified as a Category III level severity (€300,000 - 750,000) which is the second most serious of the four levels. The basic fine was €525,000, but the actual amount of fine was reduced by €50,000 because of Booking's effort to mitigate the damage (pertaining to 7(c)). After the investigation of its Security team, Booking informed customers of the incident and ways to limit damage to them. It also offered financial compensation to anyone who is affected or to be affected. Although AP found the incident to be serious (pertaining to 7(a) as a data breach incident with 4109 data subjects and 22 days late notification) and culpable (pertaining to 7(b), considering that Booking could have responded immediately at least to the email received on January 13 and made a conditional notification according to Article 33(4) of GDPR [2]), it did not increase the amount of fine imposed on Booking. [1]

2.3 The Disagreement

Although Booking did not appeal to the decision, there had been some disputes between Booking and AP about whether Article 33(1) is applicable to this incident before AP made the decision. First, Booking claimed that it wasn't aware of the personal data breach until February 4. However, AP pointed out that there were several emails sent from Trip Advisors which made Booking possible to be aware of the situation. Booking also could have taken advantage of supplement initial notification later to AP according to 33(4) of GDPR.

Booking also pointed out that since customers' email addresses are hashed on Extranet, Booking concluded that the breach was not caused by its system before receiving more subsequent emails from Trip Providers. AP did not accept Booking's position since Booking did not follow its internal security protocol to contact Security team directly whenever there is a suspected security threat, but Security team was not involved until January 31. Also, the cyber-criminals knew some details of data subjects' reservation details, so Booking should have sensed the necessity to report to the supervisory authority, which is AP in this case.

While Booking acknowledged the fact that it is the data controller for customers in relation to its platform, it stated that Trip Providers also act as data controllers for customers whose data are accessible to Trip Providers via Extranet. AP concluded that Booking is the sole data controller since Booking defined purposes and data types in its policy, had been responsible for security of Extranet, and submitted a report to AP about the breach alone.

3 Significance

The incident followed by AP's fining is noteworthy since it records the biggest fine issued to a company only with late data breach notification. [5] Other than this incident and fining on Twitter by Ireland on December 15 2020, publicly announced fines related to only late date breach notification has not exceeded €70,000. The Dutch DPA has been emphasizing the obligation of data breach report through provision of ample information and extensive press release, resulting in the top number of data breach notification in Netherlands among Europe. [1, 6] This incident is the first precedent of imposing Article 33(1) strictly, as previous incidents such as the cases of Mariott and British Airway on 2018 were treated relatively leniently. [5] This may serve as the beginning of the new trend in the EU toward handling violations of data breach notification strictly. However, there are still only six cases on [7] related to data breach notification imposed after the decisions for Booking and Twitter, where all six cases were investigated only by the Polish DPA. Although this may be the evidence that companies are abiding by the obligation of notification better, it seems to me that the disagreement between European Data Protection Supervisor and AP on the severity of late notification as mentioned in [1] has not been resolved yet.

Although Booking acknowledged its mistake of late data breach notification, it emphasized the fact that the leakage of private data was irrelevant to security practice in Booking's system. [5] Indeed, the attack was clearly non-technical and labeled as a "social engineering" attack by AP. [1] However, it is clear that even the attack was not technical, the system indeed had its weak points even if it was not part of Booking itself. If Booking decided to share Extranet with Trip Providers, the engineers of the system had to make sure that socially engineering attack cannot happen by further authentication method or reminding representatives of Trip Advisors sufficiently. The incident shows that privacy-secure systems definitely need to take account users' inadvertent behaviors and mitigate damage caused by them.

References

[1] AP booking.com B.V.
https://gdprhub.eu/index.php?title=AP_-_booking.com_B.V.

[2] General Data Protection Regulation.
https://gdpr-info.eu.

[3] Dutch DPA Updates Policy on Administrative Fines.
https://www.huntonprivacyblog.com/2019/03/26/dutch-dpa-updates-policy-on-administrative-fines/.

[4] Boetebeleidsregels Autoriteit Persoonsgegevens 2019.
https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/03/stcrt-2019-14586.pdf.

[5] Is the Amount Excessive? Hefty Fine for Booking.com Due to Delayed Data Breach Notification; With Little Financial Information Stolen.
https://www.cpomagazine.com/data-protection/hefty-fine-for-booking-com-due-to-delayed-data\-breach-notification-with-little-financial\-information-stolen-is-the-amount-excessive/.

[6] Double Dutch: Netherlands tops GDPR breach report index for second year running.
https://portswigger.net/daily-swig/double-dutch-netherlands-tops-gdpr-breach-report-index-for-second-year-running.

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