GDPR Case Study: World Trade Center Bucharest (Romania)

Marilyn George
mgeorge5

Abstract

The World Trade Center Bucharest was fined 71028 lei (15,000 euros) in July 2019 for exposing 46 guests' personal information in an easily accessible manner.

1 Introduction

In July 2019, the Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP) concluded the GDPR investigation of a data breach reported at the World Trade Center Bucharest [2]. The incident concerned the personal data of 46 guests at a hotel owned by the entity. The guests' names and personal information were on a printed list that was used to verify breakfast guests at the hotel. This list was photographed by individuals outside the organization, and subsequently pictures of the list appeared online [5].

2 The Violation

Background. The data subjects in question were 46 guests[1] at a hotel owned by the World Trade Center in Bucharest, Romania. Their data was available to the hotelier (data controller) which gave data access to its employees (data processors). The responsible authority was the Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP), which was handing out its second fine under the GDPR.

What? Hotel employees were using pen and paper to verify the guests who were attending breakfast at the hotel. For this purpose they had a printed list of the guests' details. We can only speculate about the contents of this list, as all the sources found only said 'personal data'. At the minimum it would have contained names and room numbers of the guests. However, hotels have access to a large amount of information about their clients; including addresses, idenfication documents and payment data. It is possible that at least some of this personal information was also part of this list. The list was photographed by outsiders and later appeared online, leading to the data breach in question.

Why? In this particular case, it would appear that a *lack of technological sophistication* was part of the reason for the breach. Employees used paper and pen lists instead of having key card scanners or any other computerized means of verifying the guests. A computer system would have been easier to secure (with credentials) than a paper list in an employee's possession. It is also possible that the paper system had been in place for a while and existing processes were not reexamined in the light of the GDPR. This could also have been due to employee oversight caused by *insufficient awareness*. Another contributing factor might have been the *seemingly trivial nature* of the process - it was only meant to check if the people having breakfast were indeed guests at the hotel. Even if the more clearly sensitive processes, like checking in or payment processing were GDPR compliant[2] and secure, it could have been that verifying breakfast guests was not even considered as a potential source of a data breach.

Fallout. Upon discovery of the breach, it appears the hotel self-reported to the ANSPDCP as per art. 33 of the GDPR [4]. The investigation discovered violations of article 32 para. 4 in relation to article 32 para. 1 and para. 2 of the GDPR, regarding the security of data processing [3]. Art. 34 para. 4 talks about "...controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller...". In this particular case the processors (employees) did not process according to the instructions from the controller (hotel). This led to "...unauthorised disclosure of, or access to personal data..." as in para. 2. The organization was also held responsible for the failure to "...implement ap-

[1] Nationalities unspecified.

[2] We note that the hotel seems to have both an explicit data privacy policy and a Data Protection Officer (as per art. 37 of GDPR) [6].

propriate technical and organisational measures to ensure a level of security appropriate to the risk...” as in para. 1. The principle of *operator responsibility* is also established in art. 24 of the GDPR where it says “...the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation...” On a broader scale it also led to the affectation of the rights to privacy and protection of personal data, guaranteed by art. 7 and art. 8 of the Charter of Fundamental Rights of the European Union and art. 16 of the Treaty on the Functioning of the European Union. On conclusion of the investigation it was fined 71028 lei, the equivalent of 15,000 euros[3] - which by some estimates is 0.2% of its revenue [1].

Prevention. In this particular case, larger computerization of processes would have helped. Access policies would have been easier to implement in software and using employee credentials would have prevented outsider access. For an organization such as a hotel, stringent access policies should have been in place. Additionally, the hotel should have examined all of its day-to-day operations to check for potential data breaches. It would also have helped to sensitize employees to the importance of the guests' personal data. On a broader note, the *incentivization* of self-reporting by data processors and controllers could help prevent such incidents in the future but we will discuss that further in the following section.

3 Discussion

This particular incident is interesting for several reasons - the particular mundane task of verifying breakfast guests gave rise to an unexpected data breach, the data in question was on paper, and the data controller self-reported the breach.

Awareness. We believe an important concern is one of awareness and being actively conscious of data privacy, no matter how unimportant the process. We tend to associate the term data breach with digital data being stolen from servers, but it needs to be part of a larger dialogue around everything we do that potentially exposes sensitive data.

[3]This works out to a little over 300 euros per customer. We cannot comment on the magnitude of the fine as there seems to be very little information about what exactly leaked in the breach.

[4]Who were also incidentally fined heavily for a violation.

Self-Reporting. In one of the sources for this report; Ana-Maria Udrişte, business lawyer and founder of avocatoo.ro, a organization that launched the first GDPR document kit in Romania[4] discusses the self-reporting of GDPR violations [1]. She says that self-reporting should somehow mitigate the penalty imposed on the organizations. There is a discussion to be had on the incentives of organizations to self-report their breaches, especially if it does not even make the judgement milder in any way. Adding in provisions to encourage self-reporting might make the shift towards GDPR compliance faster - with organizations working not only to comply but also to find existing flaws before someone else does.

References

[1] European premiere, the first fine applied to a gdpr consulting company. https://dpo-net.ro/european-premiere-the-first-fine-applied/-to-a-gdpr-consulting-company/. Accessed: 2019-08-18.

[2] Gdpr enforcement tracker. http://www.enforcementtracker.com/. Accessed: 2019-08-18.

[3] A new amendment in the application of the gdpr. https://www.dataprotection.ro/?page=O_noua_amenda_GDPR&lang=ro. Accessed: 2019-08-18.

[4] Regulation (eu) 2016/679 of the european parliament and of the council (general data protection regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e3722-1-1. Accessed: 2019-08-18.

[5] Romania: Dpa fines hotel 15,000 eur for not protecting list of breakfast guests. https://www.privacydesign.ch/2019/07/11/romania-dpa-fines-hotel-15000-eur-for-not/-protecting-list-of-breakfast-guests/. Accessed: 2019-08-18.

[6] World trade center bucharest privacy policy. fiȘĂ de informare cu privire la prelucrarea datelor cu caracter personal. http://wtcb.ro/PrivacyPolicy.pdf. Accessed: 2019-08-18.