GDPR Case Study
PwC fined by HDPA

Yuchen Yang
Brown University

1 Introduction

On July 26, 2019, Hellenic Data Protection Authority (HDPA) [6] imposed its first and only [1] GDPR fine against the company PricewaterhouseCoopers (PwC) [7]. PwC is fined 150,000 Euros for breach of art. 5 par 1 & 2, art. 6 par 1(a), art. 13 par 1(c) and art. 14 par 1(c) of General Data Protection Regulation (GDPR) [2]. The case was following a complaint by the Association of Auditors of the Attica Region against PricewaterhouseCoopers Business Solutions S.A. which is the PwC office in Greece. PwC used the inappropriate legal basis of consent for the processing of employees' personal data, processed the data in an unfair and non-transparent manner and transferred the burden of proof of its compliance to the employees deliberately [4]. HDPA thus order the company to correct the behaviors and restore correct applications of GDPR. At the same time, an additional fine of one hundred and fifty thousand Euros is imposed according to art. 58 par 2(i) and art. 83 of GDPR.

2 Background

In this case, the personal data of PwC employees in the Greek office is mishandled and exposed. The data subjects are the PwC employees. Both the controller and processor of the data is PwC.

PwC as one of the Big 4 auditors, is the second biggest company providing assurance, tax and consulting services for other business companies [10]. The case involves the business of Greek customers and possibly some customers in other countries. It exposes the personal data of the employees in a large range and greatly violates the privacy rights of the employees.

The case is happening in Greece and Hellenic Data Protection Authority which is the Greek national data protection authority should be the responsible data protection agency.

3 GDPR violation

The conclusion of the HDPA includes [4]:

- Unlawful processing of personal data against art. 5 par 1(a) of the GDPR.
- Unfair and non-transparent manner of processing data against art. 5 par 1(a)(b)(c) and processing under a different legal basis against art. 6 par 1(a).
- Unable to demonstrate compliance with art. 5 par 1 and transferring the burden of compliance proof to the data subjects against art. 5 par 2.

3.1 What happened?

The case first happens as PwC in Greece gives the individual contract attached to a copy of agreement to share data towards the company [9]. The details in the agreement claims that the shared data includes the information of the information collected by PwC in the past and the data in the current system. This represents that the data could possibly go to some third-party companies, and even their customers.

According to the reports of PrivSec, PwC unfairly and non-transparently processed the personal data [5]. PwC also gives its employees the false impression that their data was being processed under the legal basis of consent, while the data was processed for the goal of reducing their clients' financial expenses. PwC also provides the false impression by hosting GDPR-related seminar [8]. By hosting seminars discussing the GDPR regulations, it aims at informing Greek companies about the requirements of the new framework but also gives its employees false idea of privacy safety.

Although PwC was responsible in capability as the data controller, it failed to demonstrate compliance with art. 5 par 1 of the GDPR [4]. Hellenic DPA also decided that PwC had violated the principle of accountability in art. 5 par 2 of the GDPR by transferring the burden of proof of compliance to the data subjects [3]. PwC uses the imbalanced relationship of employer and employees to halfly enforce the agreement.

The complaint was sent by the Association of Auditors of the Attica Region and the complaint describes the situations among employees in detail. However we can't track the exact time and condition of the complaint.

The amount of the fine is 150,000.00 Euros while the net turnover during the period from July 1, 2017 to June 20, 2016 was 41,936,426.00 Euros.

3.2 Who is responsible?

PwC is responsible since they didn't have a good system of internal data protection. Although the action was designed to get more benefits for their clients, but this actually exposed important personal data of its employees and impacted their privacy security. The non-transparency of their actions and processing under different legal basis are intolerable.

Employees are victims but they should still improve their awareness of privacy-related issues.

3.3 What could have prevented this?

There are some possible technologies to prevent this.

The storage of personal data of employees should be encrypted at rest. The data should only be accessed when necessary and the priviledge should be limited to a small group of people.

The office in Greece shouldn't have such high privilege to access the employee data of their office. The headquater of PwC should develop personal encryption to enable only personal access and HQ access of the data.

The storage of the personal data should not be set at local level. It should be stored in a distributed way. The storage should only be managed by the headquarter themselves or trusted third-party data centers with self-developed encryptions.

The HQ of PwC should develop better procedures of data collection and encryptive systems for such possible issues. The process of signing individual contracts should also be standardized. No attachments should be allowed and things can go extreme under the imbalanced employment relations.

4 Discussion

In the final decision [4], it mentions that there was no need to examine the rest of the principles set after the unlawful actions found till now. It's obvious that apart from art. 5, 6, 13, 14, 58, there are some other ones PwC violated.

According to art. 83 [2], the fine was much lower than the standard. 2% of their yearly turnover is about 5 times of the actual fine amount.

As the only case under GDPR regulations processed by Hellenic Data Protection Authority, this case is pretty new and doesn't have too much information. However, we can still see that the complaint is processed but not in a strict way. This is also reasonable since it's their first case.

The case is surely significant as the first case in Greece. The fine is lower than standard but still reminds other organizations to focus more on data protection.

References

[1] enforcementtracker. Gdpr enforcement tracker.

[2] eur.

[3] fifthstep.

[4] HPDA. Hdpa decision 276/2019.

[5] Meera Narendra. Pwc fined 150,000 euros by hellenic data protection authority, Jul 2019.

[6] PORTAL1. Hellenic data protection authority.

[7] PricewaterhouseCoopers. Us pwc.

[8] pwc. seminar.

[9] secnews. Pwc fined 150,000 against gdpr by hellenic data protection authority.

[10] wikipedia. Pricewaterhousecoopers, Sep 2019.