Bergen municipality infringement of GDPR

Amir Ilkhechi (ilkhechi@cs.brown.edu)

Abstract

The Norwegian Data Protection Authority (DPA) issued a warning against Bergen Municipality on Dec 17, 2018 that it will exercise its corrective authority (GDPR Article 58.2(d)) and issue a fine (GDPR Article 83). The warning was about Bergen Municipality's infringement of data security requirements (mentioned in GDPR) which includes making a file of 35000 students and employees username and email addresses and making it openly available to students, employees and other personnel. The DPA which was the Norwegian Supervisory Authority, Datatilsynet, set the amount of fine to 170,000 euros for the infringement of the EU General Data Protection Regulation. Datatilsynet established that the municipality did not make sufficient efforts to deploy proper security measures and as a result it had violated Articles 5(1)f and 32 of the GDPR.

1. Background

To begin with, most of the information in this report has been adopted from Signatu blog [1] and iapp.org [2].

In this case study, subjects are students and employees who used eFEIDE which is a cloud service login solution used by primary schools in Bergen in order to allow teachers and students access different systems such as *Learning* which is a platform with instructors' feedback and assessments, and private communications between students and instructors.

The data controller in this case study is Bergen municipality. The data processor is Identum who delivered eFEIDE service.

The responsible data protection agency was the Norwegian Supervisory Authority, Datatilsynet [3].

2. GDPR Violation

On May 15, 2018, when the previous data protection act was in force, a school employee reported to IT department of Bergen municipality that several files that included the user-names and passwords of students and employees were accessible for students. This breach was initially discovered by a student who had reported the problem to the school employees but the school did not follow up with any security measures.

All employees and students were able to access information about all the users of the FEIDE that belonged to the Bergen municipality. The school used such files to migrate data between different systems.

2.1. What happened?

Each year at the start of the new academic year, new users were added, and by the fall break, all passwords were marked obsolete to require every user to choose a new password after the fall break. The existing passwords, however, could be used for a second time and users could use the previously used passwords after the break.

After June 22, 2018 a malicious person with a Bergen municipality user account had accessed eFEIDE and changed the contact information for the customer relationship to Identum which was discovered by Identum in August 13, 2018.

On August 14, 2018, a student logs into the Learning platform with dean's account and send messages to the other students. The message contained the dean's password.

After the incident was reported to the police, the perpetrator claimed that they were just able to have guessed the dean's password. Right after that event, Identum nullified all the admin and user accounts in mid August. Consequently, Identum sent and offer to

Bergen municipality suggesting to use two factor authentication of students and employees to login using eFEIDE.

By August 17, 2018, the incident had media coverage, and as a result Bergen municipality introduced two-factor authentication to access the user administration accounts only.

Since the infringement was discovered was before the GDPR entered into force in Norway, this case is a bit more complicated. Paragraph 33 of the Norwegian Act on data protection (personopplysningsloven) mentions that only the established rules relevant to the time of the infringement should be applied.

However, referring to the European Convention on Human Rights Article 7, the DPA concluded that the infringing act is the act that continues until the controller terminates the infringement and given that Bergen municipality ended the infringement in August 2018, it is after the time GDPR entered into force in Norway. As a result, GDPR applies to this case.

The violated sections by Bergen municipality are in Article 5 of GDPR, in particular Article 5.1(f), Article 5.2, and Article 32.1(a) and (b).

Eventually, Bergen municipality was fined 170,000 euros for their violation.

2.2. Who/what is responsible?

The Bergen municipality is responsible for this because they failed to use preventive/protective measures such as two factor authentication on all types of user account.

2.3. What could have prevented this?

If the Bergen municipality reported this incident on time and also if they had taken the security recommendations more seriously, then that fine could be avoided. Also, the municipality should educate the schools and other subordinate organizations about the security and privacy threats. The school should have reported the data breach immediately to the municipality in order for serious actions to be taken accordingly.

3. Discussion

First of all, one of the most interesting things that I learned from this case study is the fact that even if the actual data infringement takes place before certain rules and regulations are established, still it doesn't exempt the violators from fines and punishments. As it is the case with this incident, the rules might mandate that the violation is still ongoing until the appropriate measures to stop the effects of the violation are taken by the data controller or the processor.

Another aspect of this case study that makes it really important is that it is concerns children and students. Therefore, it should be taken more seriously and I think that the imposed fine is well justified and fair.

Although it may sound like a rare GDPR violation incident, I believe that similar infringements happen in other schools and small organizations partly because of the lack of knowledge in management levels and also a shortage of IT personnel who are familiar with GDPR rules. Another reason can be that the current hardware/software is innately prone to mistakes that may result in catastrophic privacy violation results.

References

1. https://blog.signatu.com/blog/2019/01/08/norwegian-dpa-to-fine-city-of-bergen-for-gdpr-breach/
2. https://iapp.org/news/a/norwegian-supervisory-authority-fines-municipality-170k-euros-for-gdpr-violations/
3. https://en.wikipedia.org/wiki/Norwegian_Data_Protection_Authority