GDPR Case Study: OLVG

Emmie He, *Brown University*

Abstract

The Dutch Data Protection Authority (DPA) fined Amsterdam hospital Stichting OLVG (OLVG) 440,000 EUR for two GDPR violations [1]. The hospital did not implement two-factor authentication for in-hospital medical data access and failed to assess data processing security on a regular basis. Following the DPA's investigation, OLVG improved its information system security [1].

1. Background

OLVG is an Amsterdam-based clinical training hospital. It provides medical care to about 500,000 patients annually [2]. According to its security and privacy policy, OLVG is responsible for securing information systems, regulating internal communication, and processing electronic patient data[2]. The DPA concluded from the Commerce Chamber registration and OLVG's privacy statement that OLVG makes decisions about the purpose of its medical data and controls the means of related data processing. Thus, under GDPR, OLVG is the controller and processor and its patients are the data subjects.

It is worth pointing out that OLVG is responsible for controlling and processing large-scale health data in its hospital system [7]. According to Article 9(1) of the GDPR, health data is considered a special category of personal data [2]. Due to the sensitive nature of the data, to avoid posing significant risks to fundamental human rights, OLVG is expected to implement an information security system that conforms to generally accepted security standards under Article 32(1) of the GDPR [7]. In the Netherlands, the Dutch standard for information security in health care has already specified general guidelines regarding appropriate practices and systems [6]. OLVG also has committed to comply with these standards according to its privacy policy [7].

In 2019, a Dutch hospital Haga was imposed a fine of 460,000 EUR by the Dutch DPA for the lack of two-factor authentication and failing to protect patients' privacy [4].

2. GDPR Violations

1.1. Reports

The Dutch DPA received two data breach reports from OLVG about unnecessary user access to sensitive medical data. They started an investigation on April 17, 2019 [7].

On May 22, 2019, supervisors of the DPA conducted an on-site investigation at OLVG. At the time, OLVG was operating under an existing information system that was implemented in 2015. Specifically, the DPA examined how employees access electronic patient data, interviewed both the management and individual employees on the data processing procedure, and carried out an audit of the hospital's processing log system [2, 3].

1.2. Violations

During the on-site investigation, the DPA found that when inside the hospital, the employee of OLVG could go to the hospital computers and use their username and password to gain immediate access to electronic patient records [7]. Since it took only one piece of factor to convince the authentication mechanism that the user had access to the information system, this method was evaluated as a one-factor authentication. Under the Dutch standard for information security in health care (NEN 7510, NEN 7512, NEN 7513), access to sensitive data should be safeguarded with multi-factor authentication [6]. Therefore, OLVG's information system was not in compliance with Article 32(1) of the GDPR, which states the controller "shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk" [8]. The DPA mentioned that the "appropriate level" in this case should mean the established standards such as those specified in NEN.

Furthermore, the DPA found that between 2018 and 2019, OLVG did not conduct a periodical review of access log files [7]. These files contain information on who accessed what patient data at what time and can help surface any unauthorized activities. OLVG had two proactive checks and eight incidental checks of its logging system over the course of 15.5 months [3]. This behavior signaled a lack of systematic review to identify abnormal data access by unauthorized employees. It, therefore, violates Article 32(2) of the GDPR, which mandates special attention when processing sensitive personal data.

1.3. Disputes

During the investigation, OLVG objected to the DPA's claim that there was no two-factor authentication. They argued that their computers were locked in a restricted physical space that required employee card scanning. And this physical barrier served as a second factor for their authentication system. However, this was rejected by the DPA because the physical restriction was considered insufficient to serve as a second factor. For example, a cleaning staff could also enter the computer room with an employee card. Additionally, DPA found that certain areas of the hospital containing computers were not fully restricted [7].

1.3. Improvements

After the investigation, OLVG connected employee card readers to their computers inside the hospital. Employees need to both scan their cards and enter their credentials in order to access patient data. This effectively equipped their information system with a two-factor authentication [7].

They also established a structural log review system to detect unusual activities in a timely manner [7].

1.4. Conclusion

On November 26, 2020, the DPA imposed a 440,000 EUR fine on OLVG for the violations. The hospital did not object or appeal [1].

3. Discussion

The GDPR purposefully provides general non-specific requirements (like "appropriate level of security") when it comes to the technical implementation of security for data processing (Article 32). In the case of OLVG, it is nicely complemented with existing regulations. To some extent, this case sets a concrete example for what kind of security implementation medical care companies should adopt. A case like this helps clarify GDPR specifications in the related industry and encourages other regions and industries to issue detailed guidelines and complementary regulations. From the initial objection reaction of OLVG, we can see the tendency of companies trying to take advantage of the ambiguity in the regulation, and this highlights the importance of regulation clarity.

What makes this case interesting to me was that less than two years ago, Dutch hospital Haga was already imposed a fine of 400,000 EUR for its inadequate security measures - specifically for its lack of two-factor authentication [4]. However, since OLVG was investigated and fined for almost the same reason, the previous case and a large amount of fine clearly didn't motivate the health care industry to make changes. Although this time, unlike Haga Hospital who is still in the process of appealing, OLVG has already accepted the fine. Perhaps, and hopefully, the OLVG case will have a positive influence on hospitals domestically and internationally.

References

[1] European Data Protection Board, "Dutch DPA fines OLVG hospital for inadequate protection of medical records," [Online]. Available: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-olvg-hospital-inadequate-protection-medical-records_en

[2] Autoriteit Persoonsgegevens, "Boetebesluit OLVG," [Online]. Available: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_olvg.pdf

[3] DLA Piper "The Netherlands: 440,000 EUR fine for hospital re. unauthorised access to medical records," [Online]. Available: https://blogs.dlapiper.com/privacymatters/the-netherlands-440000-eur-fine-for-hospital-re-unauthorised-access-to-medical-records/

[4] Autoriteit Persoonsgegevens, "Haga beboet voor onvoldoende interne beveiliging patiëntendossiers," [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers

[5] Dentons, "Supervisory framework of the Dutch Data Protection Authority (DDPA;Autoriteit Persoonsgegevens)," [Online]. Available: https://www.dentons.com/en/insights/articles/2021/may/18/supervisory-framework-of-the-dutch-data-protection-authority

[6] Jacintha van Dorp, "Prevent data breach? Points of attention for healthcare providers & ICT suppliers," [Online]. Available: https://solv.nl/en/blog/prevent-data-breach-points-of-attention-for-healthcare-providers-ict-suppliers/

[7] GDPR Hub, "AP - Ziekenhuis OLVG," [Online]. Available: https://gdprhub.eu/index.php?title=AP_-_Ziekenhuis_OLVG

[8] General Data Protection Regulation, “Art. 32 GDPR Security of processing,” [Online]. Available: https://gdpr-info.eu/art-32-gdpr/