CSCI 2390 Privacy-Conscious Computer Systems - GDPR Case Study
10 September 2019, Morele.net Sp. z o. o., Poland

Zhiyuan Lai
Brown University

Abstract

The General Data Protection Regulation (GDPR) is a data protection regulation of the European Union (EU). The main purpose of this regulation is to give control to individuals (otherwise referred as data subject in GDPR) over their personal data. GDPR takes effect since 25 May 2018 [1].

In this case study, we will examine a GDPR violation by the company Morele.net Sp. z o. o. based in Poland. Morele.net Sp. z o. o. suffered **three** breaches which resulted in unauthorized access to personal data of its customers. Morele.net Sp. z o. o. was fined €660,000 (PLN 2,830,410) by Poland's Personal Data Protection Office (UODO) on 10 September 2019 for breaching Artical 5 (a) and (f), 6, 7, 24, 25 and 32 of the GDPR [6, 21]. This is the largest fine levied in Poland to date for infringement of the GDPR [16].

1 Background

Morele.net Sp. z o. o. (Morele.net Group) is a Polish-based company that opperates various online stores for buying and selling a wide variety of items such as electronic devices, toys, cosmetics, pet accessories and food supplies, sports equipment, clothing and furniture. Specifically they own and manage morele.net, hulahop.pl, amfora.pl, pupilo.pl, trenuje.pl, motoria.pl, digitalo.pl, ubieramy.pl, Mebleuje.pl, sklep-presto.pl, and buduje.pl.

Morele.net Group has a very broad user base and approximately 2,200,000 (two million two hundred thousand) unique data subjects' data have been processed by the company. The scope of this data includes name, surname, e-mail address (e-mail), telephone number, PESEL number, series and number of an identity document, date of issuance of an identity document, expiry date of an identity document, education, registration address, correspondence address, source of income, monthly net income, household costs, number of dependents, marital status, amount of other monthly liabilities in financial institutions and many more [6].

Morele.net was the target of three breaches in which about 2.2 million records were accessed by an unknown perpetrator(s) to the store's customer database, including about 35,000 records of sensitive information obtained in loan applications [19]. The stolen information was then used by sending text messages on behalf of the store to customers, demanding an extra payment to finalize their transaction and redirecting them to a bogus payment site to steal extra information such as bank authentication data [6].

2 GDPR Violation

2.1 What Happened - Timeline of Events

Morele.net was informed by customers in November 2018 that they had received short text messages (SMS) telling them of the need to pay an additional PLN 1 charge to finalize the transaction. The message contained a link to a fake electronic payment gateway. The company reported the incident to the police immediately and sought to clarify the matter. An investigation was carried out by the Morele.net and two breaches of personal data protection was found.

Morele.net subsequently received an e-mail from an unknown entity informing them of the theft of the customer database and threatened to release the information collected on the web in return for ransom money. Morele.net did not pay the hackers and reported the violation to the UODO about the alleged unauthorized access customer database where approximately 2,200,000 users affected. The hackers then published the stolen database records online [19].

Morele.net reach out to its 2,200,000 customers through e-mails [17] in December 2018 informing them about the breach. The customers were also told that Morele.net does not process data from loan applications. In the same month, Morele.net found another unauthorized access to its system and personal data such as ID card details, financial situation like source of income, monthly net income, costs of living and maintaining a household, number of dependents, marital status and sum of financial obligations were accessed. Around 600 data subjects were identified and told of the incident. The violation was reported to UODO.

In January 2019, due to the fact that the notification of data subjects did not meet the criteria set out in Article 34 of GDPR, the president of UODO ordered Morele.net to re-notify the data subjects of the breach of their personal data, advising them on how to minimize the potential consequences of the breach. In response, Morele.net resend a notice to 35,000 affected customers again [6].

2.2 UODO's Notice

Following UODO's investigation, it was concluded that the organizational and technical data security measures used by Morele.net were insufficient to the existing risk related to the processing of their customer data. Particularly, Morale.net failed to react and respond to the emergence of unusual traffic on its network, resulting in the breach. Moreover three basic infringements were listed in the UODO's decision:

1. Morele.net did not comply with the Article 5(f) and Article 32 (1) of the GDPR, principle of confidentiality, as defined in the GDPR.

2. Morele.net did not effectively monitor potential threats, especially those related to unusual online activity. Morele.net did not react and respond fast enough when it became clear that large amounts of data were being downloaded.

3. Morele.net states that it processed data on the basis of consent obtained from users, however Morele.net was unable to provide proof that it had obtained consent from data subjects for such processing [6]. Article 7 of the GDPR, accountability principle of the GDPR, was therefore violated as well.

Due to the high risk of adverse consequences for more than 2 million data subjects, Morele.net was fined more than PLN 2.8 million (EUR 660,000) for inadequate protection of personal data and for various GDPR violations.

2.3 Morele.net's Appeal and Final Verdict

In response to the enforcement notice, Morele.net appealed against it. Morele.net reported that the company had engaged external firms to perform regular security audits to verify the system's security and had deleted the database which stored loan information provided by data subjects [6].

The inquiries carried out by the Authority, however, found that there were insufficient security measures in place. Moreover, Morele.net was unable to prove that it had obtained consent from data subjects before storing their financial information on its database. The two major security failures highlighted by the Authority with Morele.net are the following:

1. Systems did not have proper access authentication processes. Only one-factor authentication was used, which is more vulnerable to security violations.

2. The monitoring of potential threats related to unusual online activities deployed by Morele.net was ineffective.

Morele.net ended up losing the year long case, as the Provincial Administrative Court in Warsaw upheld the fine of over PLN 2.8 million levied on Morele.net [13].

3 Discussion

3.1 Significance of the Case

The decision made by UODO highlighted UODO's stance on the importance of effectively monitoring potential risks, as well as implementing appropriate safeguards for protecting databases. According to Article 32 of the GDPR, it states that one of the aspects to be taken into account when deciding on implementation of technical and organizational measures should be the state-of-the-art [1]. UODO states that these measures should be assessed and analyzed by taking into account market conditions, in particular the availability and market acceptability of a given technical means. UODO also notes that guidelines in that regard are provided by applicable standards, in particular ISO standards, are subjected to constant reviews and changes conditioned by technological progress [6]. UODO included several examples of notable sources [4, 7, 9, 14, 15, 18].

UODO's statements help existing and new data processors to better understand the viewpoint of the concept of "state-of-the-art" according to UODO and the standards to adhered to / followed so as to comply with the GDPR.

Furthermore, the record fine of €660,000 (PLN 2,830,410) imposed on Morele.net may serve as a deterrent against violation of GDPR. Data controllers are discouraged from violating personal data protection provisions where the penalties for such violation(s) would be hefty [16].

3.2 Accountability

Morele.net's decision to perform deletion of a database which stored unconsented customers' loan application data for auto-filling purposes was clearly a violation of the basic principles of personal data protection. Furthermore, there was no prior analysis and / or proper documentation of the deletion process. However, even though these personal data were processed before the enforcement of GDPR, data controller was still held accountable for any GDPR violation.

3.3 Term "Large" Scale

The GDPR does not define what constitutes large scale processing. It is interesting to point out that UODO mentioned

that the processing of 2,200,000 data subjects' personal data should be treated as processing on large scale [6]. While there isn't an offical definition or criteria to the term "large scale" processing in GDPR, this case has certainly helped data controllers (in Poland) to better understand UODO's definition of the term "large scale" and they can determine on whether the "large scale" GDPR factor applies to them.

3.4 Was the Fine Imposed Appropriate?

A fine of over PLN 2.8 million (EUR 660,000) was imposed on Morele.net Group for the violation of GDPR where over 2 million data subjects' personal data was compromised. This amount to roughly PLN 1 per record.

According to the personal data worth calculator [20], the cost of a personal data for the above-mentioned data scope 1 is USD 0.1191 which is about PLN 0.47, and login credentials such usernames and passwords cost USD 0.55 [11], which is equivalent to PLN 2.15. The total value of a data subject's personal data is roughly PLN 2.5 which is more than twice the fine imposed. In addition, the reported annual revenue of Morele.net in 2018 was USD 131.0 million [3] which is equivalent to PLN 512,511,300.00.

Under GDPR, the maximum fine for GDPR violation is €20 million or 4% global annual turnover [1]. The fine imposed on Morele.net was roughly 0.5%. Thus, in my opinion, I would argue that the imposed fine was rather lenient and should have been more given the scale of the data breach and the number of violations of GDPR.

3.5 Security Standards - What Could Have Done better?

Pertaining to the two key failures identified by the Authority:

1. One-factor authentication - Morele.net should place emphasis on data protection by following security recommendations or ISO standards adopted by the industry and use two-factor authentication instead. One-factor authentication is out-dated.

2. Ineffective monitoring - One way to circumvent this is to deploy an Intrusion Detection System (IDS) to highlight suspicious activity. Moreover, the company could have adopted a more proactive approach by hiring external firms to pentest their systems on a regular basis to identify vulnerabilities and patch them.

In addition, customers' login password stored in the database were MD5 hashed (information of whether it was salted is not available) [2, 12] where by the hashes generated by MD5 algorithm are prone to collision [5]. MD5 algorithm is also known to be the least secure hashing algorithm as compared to the current security standard recommended by security oragnizations [8, 10]. OWASP categorized MD5 algorithm as a legacy algorithm.

References

[1] European Commission. Reform of eu data protection rules, May 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[2] Cyberologue. Cyberologue - actualité cybersécurité, rgpd, réputation, 2019. https://www.facebook.com/Cyberologue/posts/morelenet-2467304-breached-accounts-in-october-2018-t635705310176373/.

[3] ECommerceDB. Morele.net revenue analytics, 2019. https://ecommercedb.com/en/store/morele.net.

[4] ENISA. Guidelines for smes on the security of personal data processing, 2017. https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-

[5] Stack Exchange. About secure password hashing, 2013. https://security.blogoverflow.com/2013/09/about-secure-password-hashing/.

[6] Office for Personal Data Protection. Infolinia urzędu 606-950-000, 2019. https://uodo.gov.pl/decyzje/ZSPR.421.2.2019.

[7] Polish Committee for Standardization. Pn iso/iec 29115, 2017. https://infostore.saiglobal.com/en-us/Standards/PN-ISO-IEC-29115-2017-952714_SAIG_PKN_PKN_2238425/.

[8] OWASP Foundation. Owasp threat model for secure password storage, 2012. https://owasp.org/www-pdf-archive//Secure_Password_Storage.pdf.

[9] OWASP Foundation. Owasp top ten 2017, 2017. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/.

[10] OWASP Foundation. Password storage cheat sheet, 2020. https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#modern-algorithms.

[11] TEGNA Inc. Your password is probably for sale on the dark web, here's how to check, 2017. https://www.wfaa.com/article/money/consumer/your-password-is-probably-for-sale-on-the-dark-web-he454770830.

[12] Gen News. Morele.net - 2,467,304 breached accounts, 2019. https://www.gen.net.uk/about-us/news/83-data-breaches/13060-2019-06-11-14-38-15.

[13] Newsbeezer. Morele.net has to pay a record fine for a major data breach. the appeal against the decision of the data protection office (uodo) was rejected, 2020. https://newsbeezer.com/polandeng/morele-net-has-to-pay-a-record-fine-for-a-major-data-breach-the-appeal-against-the-decision-of-the-data-

[14] NIST. Nist 800-63b, 2017. https://www.nist.gov/itl/tig/projects/special-publication-800-63.

[15] Polski Komitet Normalizacyjny. Pn-en iso/iec 27001:2017-06, 2018. https://sklep.pkn.pl/pn-en-iso-iec-27001-2017-06p.html.

[16] Agnieszka Nowak-Blaszczak and Monika Gaczkowska. Poland: Eur 660,000 fine in poland for violation of personal data protection regulations, 2019. https://www.mondaq.com/data-protection/848252/eur-660000-fine-in-poland-for-violation-of-personal-data-protection-regulations?

[17] Editorial Office. Morele confirms that customer data has been stolen, 2018. https://niebezpiecznik.pl/post/morele-potwierdza-ze-wykradziono-dane-klientow/.

[18] CERT Polska. Security landscape of the polish internet, 2018. https://www.cert.pl/wp-content/uploads/2019/09/CERT_Polska_report_2018.pdf.

[19] Daria Rutecka. Increased activity of the polish data protection authority, 2019. https://www.schoenherr.eu/publications/publication-detail/increased-activity-of-the-polish-data-protection-authority/.

[20] Financial Times. How much is your personal data worth?, 2013. https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2z2agBB6R.

[21] CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB. Gdpr enforcement tracker. https://www.enforcementtracker.com.