The First GDPR Fine Imposed by the Government of Poland

Yanyan Ren
Brown University

1 Introduction

On March 26, 2019, UODO (Polish abbreviation for Personal Data Protection Office) issued a news article on their website, announcing the first GDPR fine imposed to a private company for their failure to fulfill the information obligation and violation of article 14. The amount of fine is 943,000 PLN, which is roughly 220,000 EUR. [2].

2 GDPR violation

2.1 What happened?

Bisnode is a Sweden-headquartered European digital marketing company that specializes in data analytics and business intelligence. Their branch in Poland had collected data from public registers and databases pertaining to 6 million business owners, in order to provide creditworthiness scores to banks [5]. The data collected include names, national ID numbers, and any legal events related to their business [7]. While gathered data for over 6 million people, Bisnode only sent email notification to 90,000 people, out of which 12,000 objected [2]. Bisnode also presented information clause on its website, as another means of notification [2].

2.2 What could have prevented this?

According to UODO, Bisnode as the data controller was aware of its obligation of providing information, but didn't properly fulfill the obligation mentioned in Article 14 (1) to (3) of the GDPR [2]. Bisnode disputed UODO's decision by claiming that high cost from notifying via phone or postal mail would count disproportionate effort (estimation of 9 million EUR [7]), which corresponds to Article 14 (5) that makes (1) to (3) no longer apply.

The main controversy here lies in the way of interpreting disproportionate effort. Does publishing a notification on the company's website count as "the data subject already has the information" (Article 14 5a)? Is high cost alone provides sufficient evidence for "the provision of such information proves impossible" (Article 14 5b)? GDPR does not provide clear answers to these questions. Therefore, a set of clear guidelines on effective notification methods and the boundary for disproportionate effort (when it counts as "impossible) could have prevented the controversy, and might have prevented Bisnode from processing data in the first place.

2.3 Who exactly is responsible?

One interesting thing to note is that in the government's press release, the name of the company and any other details that would expose the identity of the company are not mentioned. Furthermore, both in the press release [2] and the decision [1], Bisnode was only referred to as either "the company" or "the controller". A spokesperson for the UODO claimed that the name of the company was not the focus of the case, since its president considered "information about the administrative fine and its justification is sufficient" [7].

Compared to most other governments calling out the names of the company [6], UODO's choice to hide the company's identity seems odd, and doesn't line up with people's expectation of transparency when it comes to GDPR. Also, the hiding wasn't effective anyway. As Olejnik described in his blog [9], reversing the pseudonymization took very little time and required no particular background knowledge.

3 Discussion

3.1 What's not talked about?

There are several limitations of this report due to lack of information. Since most press releases and articles on this case focused on it being the first ever GDPR fine imposed in Poland, they omitted the details of the beginning and the end of the event. It was challenging to find out who caused the action to be taken – whether a customer complained or UODO

Company	Country	Date of Fine	Fine	% of Annual Revenue	% of Maximum Possible Fine
Knuddels	Germany	November 2018	€20000 (£17,500)	0.27	0.10
Google	France	January 2019	€50m (£44m)	0.04	1.02
Taxa4x35	Denmark	March 2019	DKK 1.2m (£140,960)	1.49	0.80
Bisnode	Poland	March 2019	PLN 944,470 (£192,500)	0.06	1.6
British Airways	UK	July 2019	£183.39m	1.41	35.21
Marriott International	UK	July 2019	£99.2m	0.60	14.98

Figure 1: A summary of selected GDPR fines (source: [4])

found out themselves. It was also challenging to find any followup – when and how much Bisnode paid, whether Bisnode notified all the remaining millions of people or deleted all its data. On Bisnode's website [3], no news article mentioned the fine; a search for GDPR returned lots of web pages on the company's dedication to comply with it, but still zero mentions this particular case.

3.2 Was the fine imposed appropriate?

As mentioned in section 2.2, there has been controversy on whether a fine should been imposed in the first place. Although Article 14 described the content needs to be included in the notification, it didn't specify the medium of notification, in particular, what counts as timely and active notification. Therefore Bisnode argued that they did notify people by posting on their website [2] and this should count as fulfilling information obligation. Instead of giving Bisnode consent to process their data, people need to explicitly object (either by replying to email or drafting an email after seeing the announcement on Bisnode's website). Not getting an objection shouldn't count as getting consent. Thus, I believe a fine should be imposed.

To put the amount of fine into perspective, we can compare it against Bisnode's annual revenue in figure 1. The fine is 0.06% of Bisnode's annual revenue. Compared to other companies in this table, Bisnode's amount is on the lower-end. Note that the penalty not only include the fine, but also the requirement to notify all impacted individuals [1]. According to Bisnode's estimation, this would cost around 8 million EUR [7], and therefore Bisnode said that it would delete the records instead [8]. Since I couldn't find any followup information 3.1, it is hard to judge what price Bisnode actually paid.

3.3 What can we do as system designers?

On the first glance, this case does not involve much technical fixes. In terms of regulating the original data, Bisnode was able to obtain its data from public available sources, therefore there is not much to do. In terms of improving ways to notify involved customers, Bisnode was well aware of their options from the beginning to contact people via phone or postal mail, they simply chose to not to go through due to the cost. In terms of providing more ways to protect customers' rights to data, people who didn't get the email notification would have no way of knowing that their data was being used.

However, if Bisnode had gotten a warning from UODO before they started processing the data about the possible violation of GDPR, maybe the warning would have prevented Bisnode from carrying out data processing. Therefore, I think that an automatic checking system will be very useful. For any company that wishes to check whether they are GDPR compliant before they start collecting or processing data, they can submit a plan that specifies the ways that data was obtained, the types of data collected, the outcomes of data processing, and the ways of notification. The automatic checking system would then check the plan against the articles in GDPR (this could work similarly as formal verification), determine whether a warning is necessary, and calculate an estimated fine. Making an automatic system might be overly ambitious, but I think it's worthwhile to consider setting up a protocol where companies can check on their possible GDPR violation before they do anything with the data.

References

[1] Decisions of the president of uodo, Mar 2019. https://uodo.gov.pl/decyzje/ZSPR.421.3.2018.

[2] The first fine imposed by the president of the personal data protection office, Mar 2019. https://uodo.gov.pl/en/553/1009.

[3] Bisnode. Bisnode official website. https://www.bisnode.com/.

[4] Mathew Broughton. The ico triple hit: Rtb ultimatum, cookie usage and record gdpr fines, Jul 2019. https://www.exchangewire.com/blog/2019/07/15/the-ico-triple-hit-rtb-ultimatum-cookie-usage-and-recc

[5] Eline Chivot and Daniel Castro. Gdpr penalties prove why compliance isn't enough-and why companies need clarity, May 2019. https://www.techdirt.com/articles/20190506/10401242147/gdpr-penalties-prove-why-compliance-isnt-enoughand-why shtml.

[6] CMS. Gdpr enforcement tracker. http://www.enforcementtracker.com/.

[7] Natasha Lomas. Covert data-scraping on watch as eu dpa lays down 'radical' gdpr red-line, Mar 2019. https://techcrunch.com/2019/03/30/covert-data-scraping-on-watch-as-eu-dpa-lays-down-radi

[8] Jolanta Ojczyk. Firma ukarana milionową karą za naruszenie rodo odwoła się do sądu, Jul 2019. https://www.prawo.pl/biznes/kogo-ukaral-uodo-za-naruszenie-rodo,391858.html.

[9] Łukasz Olejnik. Anonimizować czy nie anonimizować decyzje uodo?, Apr 2019. http://prywatnik.pl/2019/04/15/anonimizowac-czy-nie-anonimizowac-decyzje-uodo/.