On the Sanction to ACTIVE ASSURANCES for Customer Data Breach

Zhoutao Lu
Brown University

Abstract

On July 25, 2019, the National Commission for Informatics and Liberties(namely, CNIL), which is the data protection agency in France, imposed the administrative fine in the amount of 180,000 euros on the insurer ACTIVE ASSURANCES due to its "failure to ensure the security and confidentiality of personal data"[6]. This amount of fine is just from the lack of basic security functionalities of its website, which prompts us to the importance of data protection in IT security[7], especially for organizations processing personal data.

1 Background

ACTIVE ASSURANCE(the company) is a simplified joint-stock company that acts as an insurance intermediary, designer, and distributor of automobile insurance policies for individuals, direct sales or online sales, and has around 160 employees[6].

Basically, the company develops insurance products, distributes them online, ensures underwriting and monitoring, manages financial flows and, sometimes, claims management[10]. With this goal, they developed the website www.activeassurances.fr for their customers to access their digital services, including obtaining a car insurance rate and take out a contract to ride, etc.[4] The customer accounts on the website contain personal information, including first and last names, postal address, email address, and telephone numbers. Besides, each account has related PDF documents, such as identity documents, quotes, certificates of automobile insurance or insurance contracts, which are stored in Microsoft Azure[6].

Throughout the case, the National Commission of Informatics and Liberties(namely, CNIL), as the data protection agency for France, decided on the actions to take, held the restricted training session and determined the final sanctions, including administrative fine and additional advertising sanctions[6].

2 GDPR violation

The investigation was initiated because of the report from a client of the company on 1 June 2018[6] that it had access to the data of other customers without authentication checks. On 27 June 2018[6], the National Agency for Security Information Systems (ANSSI) also reported they can access users' personal data without authentication checks from the search engine Duckduckgo (https://duckduckgo.com).

2.1 The lack of security for personal data

To verify the company's compliance with the law on information technology, data files and civil liberties[3] and GDPR regulation[9], NCIL carried out an online monitoring mission by a delegation on 28 June 2018[6], the second day of ANSSI's report. From the monitoring mission, the delegation noticed that a search request on Duckduckgo with the keywords "client.activeassurances.fr site: client.activeassurances.fr" returns hypertext links to certain customer accounts of the company, through which all the information and related documents can be accessed without prior authentication. The doc-

uments and customer data were also accessible by changing the numbers at the end of the URLs displayed in the browser[1].

The company did not deny its lack of security on the website which led to the breach of personal data. It violated Article 32(1) of GDPR "*Taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purpose of the treatment and the risks, the degree of probability and severity of which varies for the rights and freedoms of natural persons, the controller and the processor shall implement the appropriate technical and organizational measures to ensure a level of security appropriate to the risk*". And Article 32(2) of GDPR also points out that "*... account shall be taken in particular of risks that are presented by , unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.*" However, the company did not take the appropriate technical and organizational measures to prevent the unauthorized disclosure of personal data.

It is obvious that the defective design of the website is the reason for this case. First, there is no authentication process while accessing personal space and thus one can access and download personal information and related documents of other customers. Second, the website did not have a directive limiting on indexing by the search engine, and thus Duckduckgo could possibly crawl the account link as the search results.

Upon informed of this issue, the company took some corrective measures, including securing the account links exposed from the search engine and encrypting the documents on Microsoft Azure. However, the company still failed to prevent the account links appearing on the search engine and some cached UI components could still access the personal information page.

This case prompts us some very basic security functionalities that a website controlling and processing personal data should have. First, the request to access personal data should be authenticated as the very first step. Cookies, tokens are the most common method to implement the authentication procedure. From a more general and advanced perspective for authentication, there are many new and changing technologies and various roles to be authenticated. Tim Moses proposed that the most cost-effective and long-term solution to user authentication includes building a flexible platform that supports various authentication technologies today, and able to accommodate new ones[8]. Second, the links to account pages should be removed from the search engine's index. Several measures to accomplish that include (1) add robots noindex meta tag:

```
<meta name="robots" content="noindex" />
```

in the ¡head¿ section of the returned HTML page; (2) add noindex directive to HTML response header:

```
X-Robots-Tag: noindex
```

; (3) add a robot.txt file which indicates accessible files, although it cannot prevent indexing when it is a reference link from another page.

2.2 The lack of robustness of the passwords

After an on-site audit at the companys premises, when the company took some measures mentioned in the previous section, the delegation also found the company required its customers to use their date of birth as the password and also this specific format is clearly declared on the login page. Worse still, when the customer creates an account, the login ID and password will send by emails and clearly indicated in the body of the message.

Considering the strong password underlined by ANSSI and robustness requirements of password, the Restrict Training considers the company's passwords for customer accounts do not satisfy the requirement. Also, the approach to send passwords in the plain text of email messages is very vulnerable to interception attacks and cannot ensure data security. Also, based on these elements, the company is considered as constituting a breach of Article 32 of the GDPR.

As suggested by ANSSI, a good password should be difficult to find again even using automated tools. Its strength depends on its length and the number of possibilities that exist for each character that composes it. One acceptable format of a good password

could be including at least 12 characters with at least one capital letter, one lowercase letter, one digit, and one special character.

3 Discussion

3.1 The amount of administrative fine

Although it looks that the breach is just from the lack of some basic security functionality, to understand this amount of fines, we need to have look at the scope of the data breach. The data breach totally affected a large number of customer personal data and documents, including 144,057 telephone numbers, 144,890 gray-card copies, 137,776 copies of driver's licenses, 119,940 bank identification records, 119,517 quotes or 36,068 copies of statements of assignment of a vehicle[6]. But fortunately, the company informed its customers of the security breach and no damage to them was brought to attention. Besides, considering the company's annual turnover according to Article 83, and the active cooperation and faith on the resolution of the issue, the restrict training decided to decrease the administrative fine from 375,000 euros to 180,000 euros. The order of administrative fine is close to the number of data affected and also based on the 2% turnover limits from GDPR Article 83, this should be an appropriate amount for the company.

3.2 The enforcement process

The CNIL listened to an individual's report and also worked with another party, namely ANSSI, to initiate the monitoring session on the company very promptly. It took around 10 months for the whole investigation and reported the initial administrative fine effectively. And for another 4 months or so, CNIL prepared the Restricting Training session, finalized the fine with the company and made the announcement on the case. From this effective process, CNIL worked with ANSSI in addition to the data subject, which prompts us that "these regulators are working more and more together."[7]

3.3 Related cases

While the case is related to failure on basic security functionalities - access authentication, it is really not alone. On Dec 27, 2018, CNIL announced the administrative fine of 250,000 euros to Bouygues Telecom due to personal data breach of more than 2 million customers for over 2 years[2]. The technical cause is that the authentication functionality was disabled during the test phase and was not reactivated. On June 6, 2019, CNIL announced the fine of 400,000 euros to a real estate service provider, SERGIC because of the failure to implement data security measures and define the data retention period[5]. On June 7, 2018, Optical Center was fined for 250,000 euros, because of the lack of verification before accessing the personal invoice. It caused more than 334,000 records compromised[4]. When designing websites, as a controller of sensitive personal data, the organization should pay the utmost attention to compliance with GDPR, ensuring that there will not be a potential risk of compromising those data.

References

[1] CNIL. Active insurance: € 180,000 sanction for breach of customer data security. https://www.cnil.fr/fr/active-assurances-sanction-de-180-000-euros-pour-atteinte-la-securite-des-donnees-des-clients.

[2] CNIL. Bouygues telecom: pecuniary sanction for breach of customer data security. https://www.cnil.fr/fr/bouygues-telecom-sanction-pecuniaire-pour-manquement-la-securite-des-donnees-clients.

[3] CNIL. The law informatique et liberts. https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf.

[4] CNIL. Optical center: sanction of 250,000 for an attack on the data security of customers of the website www.optical-center.fr. https://www.cnil.fr/fr/optical-center-sanction-de-250000eu-pour-une-atteinte-la-securite-des-donnees-des-clients-du-site.

[5] CNIL. Sergic: 400,000 sanction for data breach and non-compliance with retention periods. https://www.cnil.fr/fr/sergic-sanction-de-400-000eu-pour-atteinte-la-securite-des-donnees-et-non-respect-des-durees-de.

[6] Alexandre Linden. Deliberation of restricted training no. san - 2019-007 of 18 july 2019 imposing a financial penalty against active assurances. https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000038810992.

[7] Vincent Manancourt. Cnil targets another company over basic security failures. https://globaldatareview.com/article/1195595/cnil-targets-another-company-over-basic-security-failures.

[8] Tim Moses. What type of authentication is best for gdpr compliance? https://www.entrustdatacard.com/blog/2017/august/what-type-of-authentication-is-best-for-gdpr-compliance.

[9] The European Parliament and The Council Of The European Union. Regulation (eu) 2016/679 of the european parliament and of the council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[10] Cambo Partners. Active assurances lbo with bpi france activa capital. https://www.cambonpartners.com/en/transactions/none-none-1527163692.34.