Brandenburg Commissioner
for Data Protection and Access to Information

Final Decision

national reference	136/20/1276, 136/20/2192
case register no.	306316
Art. 56 procedure	143055
draft decision	306327
Revised draft decision	437344

I. Data breach description

The controller reported two personal data breaches pursuant to Article 33 of the GDPR in July 2020 and December 2020. The cause of both personal data breaches and the resulting notifications was based on a software error.

The first software error occurred in connection with the social login and was discovered by two German users who reported the error to the responsible party. A potential attacker would first have had to log in to the user's account with a correct username/password combination via a social login. The browser stores a token that would have confirmed the successful login with the social login at [redacted]. Then a potential attacker would have been asked for the name of the other person during an account change. If the attacker knew the username of another user and entered it during the account switching process, he could have logged into the other account. The software bug did not affect two-factor authentication. The discoverers of the bug accessed accounts from two commercial accounts for testing purposes, so the affected parties of the personal data breach in question are the two commercial sellers. Beyond that, no other affected parties are known. However, [redacted] assumes that the bug had already existed since 2018. The bug was reported on November 17, 2020 and directly fixed. A report to the responsible supervisory authority was obsolete at that time, because it was assumed that the bug occurred on the same computer of both discoverers. Therefore, after evaluating the bug and its scope, the notification was made on December 9, 2020. Successful inspection by the discoverers of the bug was made on the public username, name and business address of the company owner, in-formation on company turnover, obfuscated and shortened phone number and email address.

The second software bug occurred because - in addition to the name - the specified residential address of commercial sellers, which had to be specified or updated as part of the customer verification check, overwrote the registered business address in the [redacted] database and thus became visible on the platform. This affected approximately 1200 - 1300 commercial [redacted] sellers from Germany. According to [redacted], the number of affected sellers corresponds to [redacted] of [redacted] users in the EU. However, there are no known affected sellers from other European countries - according to [redacted], only German sellers are affected. The facts of the second software error are nevertheless the subject of this decision due to the similarity to the first software error.

II. Measures by [redacted] / risk assesment by [redacted]

In general, [redacted] has a comprehensive process for software development and testing. In particular, a "Software Development Life Cycle" (SDLC) process runs through various tests such as user acceptance tests, unit tests or functional automation tests. A final approval of the testing is given by QoS engineers. In addition, a release goes through a [redacted], in which a global information security team is significantly involved and decides on the subsequent implemen-tation and testing and evaluation of the test results. Furthermore, [redacted] is com-mitted to (further) automating tests.

The cause of both software bugs was an error within the design and test phase of the software development cycle. The wrong data source was accidentally used for the application. There were also no noticeable bugs during the quality as-surance process or during the "production smoke tests".

As an immediate measure, all current projects were stopped and an investigation into the cause of the error was initiated. [redacted] assured to improve the software development process and especially the internal control of access to data. In addition, the API responsible for access would be improved and an immediate compulsion to call the API would be enacted.

III. Legal assessment

a. Decision of the Brandenburg Commissioner for Data Protection and Access to Information from June 7, 2021

We closed our first legal assessment with the following conclusion:

„Due to the measures taken immediately, the general measures within the meaning of Art. 32 of the GDPR and the fact that the Brandenburg Commissioner for Data Protection and Access to Information has not received any complaints within the meaning of Art. 77 of the GDPR for either software error, we consider the matter closed.“

b. Objection / comments by SA Poland

The SA Poland raised an objection to our draft decision from June 7, 2021.

SA Poland sees a violation of Art. 24 (1), 25 (1), 25 (2), 32 (1) and 32 (2) GDPR.

In the opinion of the Polish SA, a reprimand – pursuant to Art. 58 (2) lit. b GDPR – should be issued to [redacted] in connection with the violation of the provisions of the GDPR.

The SA Poland asks for the data on which the controller found the data breach and the date on which the competent supervisory authority was notified of each of the breaches. In this context the SA Poland asks for an assessment in regard to whether or not the controller has complied with Article 33 (1) GDPR.

The SA Poland also ask to indicate if the controller complied with Art. 34 (1) GDPR.

c. Revised Decision of the Brandenburg Commissioner for Data Protection and Access to Information

The Brandenburg Commissioner for Data Protection and Access to Information also sees a violation of Art. 24 (1), 32 (1) and 32 (2) GDPR because even there was a human error, further effective measures should have been taken to prevent the resulting data breach. Because of this structural error, the Brandenburg Commissioner sees an infringement.

The reason why we have not issued a reprimand in accordance with Article 58(2)(b) of the GDPR in the first place is that the SA Brandenburg is prohibited by national law (see § 43 (4) BDSG (Federal Data Protection Act)) from using the information made available by the controller in the context of the Art. 33 (1) GDPR notification.

After review of this case in the light of the RRO by the Polish SA and the second legal assessment we concluded that a reprimand according to the GDPR in the light of our national law is possible. For this reason the Brandenburg Commissioner will issue a reprimand.

With regard to the notification period within the meaning of Article 33 (1) GDPR, we were unable to identify any violation, as the period was within the 72 hours.

Since only name and email address were affected within the data breach, we do not assume a high risk in terms of Art. 34 (1) GDPR.

Since no further objection within the meaning of Article 60(4) GDPR was raised, we issue the administrative act of reprimand within the meaning of Article 60(5),6,7 GDPR and inform the data controller.

On behalf of the Brandenburg Commissioner for Data Protection and Access to Information,
September 29, 2022
Kleinmachnow, Germany