DATATILSYNET

Too Good To Go ApS
Landskronagade 66
2100 København Ø
Danmark

Sent with Digital Post

13 April 2021

J.nr. 2021-7329-0018
Dok.nr.
Sagsbehandler
[redacted]

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Concerning personal data breach

The Danish Data Protection Agency hereby returns to the case where Too Good To Go ApS, hereinafter TGTG, notified a personal data breach to the Danish Data Protection Agency (DPA) on 10 January 2020. The notification has the following reference number:

a2ef4877733f7e424e93e63235d7dcc834e2ada2.

1. Decision

After examining the case, the Danish Data Protection Agency considers that there are grounds for **issuing the reprimand** to the fact that the processing of personal data by TGTG did not comply with the rules laid down in Article 32(1) of the GDPR.

The following is a detailed examination of the case and a statement of reasons for the DPA's decision.

2. Facts

On 10 January 2020, TGTG notified a personal data breach to the Danish Data Protection Agency.

It appears from the notification that TGTG was subjected to a credential stuffing attack, in which hackers have been given access to profiles of 13.000 users residing in 12 EU Member States and Switzerland. Profiles come from an App, where TGTG connects consumers to restaurants that would like to sell the remaining food at the end of the day in order to reduce food waste.

It is apparent from the documents that on 8 January 2020 the TGTG experienced a low-frequency attack from a single IP address, which, immediately after blocking, turned into a high-frequency bot-net credential stuffing attack. According to the TGTG, out of the approximately 500.000 login attempts, botnets managed to access about 13.000 profiles, where hackers could access personal data in the form of username, e-mail, country, telephone number, purchase history and the last 4 digits of payment cards.

The TGTG has further stated that the app does not store location data, credit card information or information on searches, preferences and allergies. On that basis, TGTG has considered

that the attack intended to verify combinations of users' email and password obtained elsewhere by hackers.

TGTG has stated, that users, whose profile was compromised with an unauthorised login, received an automatic email about the incident. TGTG also logged out such users and sent an instruction on how to reset their password.

TGTG has further stated, that prior to the incident TGTG had implemented an alert for an increased server activity and for a high number of failed login attempts, followed by a manual rejection of certain IP addresses.

TGTG also has stated, that users' passwords are individually salted and b-crypted before being stored in an encrypted database, in a way that prevents any hackers from accessing or retrieving lists of TGTG users with email + password combinations in a "Password List Attack".

Finally, TGTG has stated that, in the light of the incident, TGTG carried out the following measures:

- automatic rejection of certain IP addresses if too many missed login attempts are detected within a certain period of time.
- an annual, independent test of the TGTG system. The most recent test was carried out in July 2020.

3. Reasons for the DPA's decision

On the basis of the information provided by TGTG, the Data Protection Agency assumes that there have been credential stuffing attacks, in which hackers had access to personal data of approximately 13.000 profiles.

On this basis, the Data Protection Agency assumes that there has been unlawful access to personal data and therefore considers that there has been a personal data breach in accordance with Article 4 (12) of the GDPR.

3.1. Article 32 GDPR

It follows from Article 32(1) of the GDPR that the controller must take appropriate technical and organisational measures to ensure a level of security appropriate to the risks involved in the processing of personal data by the controller.

The controller is thus under an obligation to identify the risks that the data subject's processing poses to data subjects and to ensure that appropriate safeguards are put in place to protect data subjects against those risks.

In the DPA's view, the requirement of adequate security under Article 32 would normally require the controller to ensure that information on data subjects does not come to the knowledge of the unauthorised persons. This implies, inter alia, that the controller must implement appropriate alarms and controls so that unusual increases in server activity can both be detected and automatically blocked.

In the light of the above, the Danish Data Protection Agency considers that, by not using automatic denial of suspicious high-frequency login trials, TGTG has not put in place adequate organisational and technical measures to ensure a level of security appropriate to the risks involved in the processing of personal data by the undertaking, cf. Article 32(1) of the Data Protection Regulation.

After examining the case, the Danish Data Protection Agency considers that there are grounds for **issuing the reprimand** to the fact that the processing of personal data by TGTG did not comply with the rules laid down in Article 32(1) of the GDPR.

When selecting a response, the Data Protection Agency emphasised that a high-frequency credential stuffing is a commonly known type of attack to exploit known vulnerabilities.

The Data Protection Agency has further emphasised that there were no special categories of personal data affected by the personal data breach, that TGTG's own set-up of the system protects users from the Password List Attack and that TGTG acted in a timely manner to stop the attack.

4. Final remarks

The Data Protection Agency notes that the DPA's decision cannot be appealed to another administrative authority, cf. Section 30 of the Data Protection Act.

The Danish Data Protection Agency's decision may, however, be brought before the courts, cf. Section 63 of the Constitution.

The Data Protection Agency considers that the case has been closed and then does not take any further action in the case.

Kind regards

[redacted]