Information and Data Protection Commissioner

[redacted]

Vs

[redacted]

COMPLAINT

Reference is made to the complaint (registered internally with file number CDP/IMI/LSA/17/2019) received from the Polish Office for Personal Data Protection concerning [redacted] ("the complainant") who is alleging that [redacted] ("the controller" or "[redacted]") breached her data protection rights, as enshrined under the General Data Protection Regulation[1] ("GDPR" or the "Regulation"). The complainant contended that the controller did not comply with her right of access request in terms of Article 15 of the GDPR within the established thirty (30) days' time frame.

From the information provided by the complainant, it transpires that she filed her right of access request on the 3rd of October 2018 and on the 5th February 2019, the date when she filed the complaint with the Polish DPA, the controller did not yet provide her with a reply.

INVESTIGATION

As part of the investigation process, on the 26th of July 2019, through an email, the Commissioner requested the controller to put forward their submissions on the allegation raised by the complainant. The submissions, that were received through an email on the 9th of August 2019, contained a letter that supposedly was sent to the complainant on the 4th of October 2018, the day after the complainant's request was received by [redacted], together with the file containing the copy of her data. As this letter was in the Polish language, the Commissioner kindly requested the controller to provide an English translation.

On the 12th of August 2019, the Commissioner was informed, through an email, that while working on the English translation, [redacted] realised that neither the letter nor the file containing the personal data was ever sent to the complainant, due to (verbatim) "*a wrong use of the security classification settings by the* [redacted]*'s employee with access to the mailbox (*[redacted]*) used to correspond with the said customer* [the complainant]". The security classification was set to be

[1] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

"*Internal only*". This setting does not allow communications to be sent outside the organization's network domain.

Following an internal investigation on this matter, the controller found out that (verbatim) *"after internal organizational changes the person in charge of this particular customer request left the company without concluding the case and ensuring that a reply was properly sent to the customer. For this reason, the file containing the list of personal data processed by [redacted] has not reach the customer, together with the usual letter sent to customer's following a Data Subject Access Request"*. The same day the error on the email setting was discovered, meaning on the 12th August 2019, in order to immediately address the incident, [redacted] sent the complainant another email apologising for the late reply, attaching a letter giving details about the processing of personal data, together with the requested information in the form of a PDF file.

On the 13th of August, the Commissioner requested a copy of the above-mentioned email and attached PDF file, as evidence that action has been taken in that regard. The copy was eventually received on the 14th August 2019.

The controller was further requested, through an email dated 19th August 2019, to put forward further submissions on the organizational and security measures implemented following this incident, to prevent such a similar incident from occurring again. From this submission, received on the 23rd August 2019, it transpires that now [redacted] has extended its backup continuity procedure to ensure that customers' requests to exercise their rights under the GDPR are addressed promptly, (verbatim) "*The procedure is designed to ensure an adequate follow-up and mirroring of the tasks within the Customer Service Unit. All the customer requests are now followed-up by two persons, one been the main contact (principal) and a second person following the correspondence as a back-up, with the capability to intervene when the principal is not capable of doing so. The principal is a senior Customer Service Agent while the "back-up" is either a Senior Team Member or a senior customer service officer having experience and knowledge on the various internal procedures regarding the types of requests received at by the Customer Services team. In case the first contact is away, sick or unavailable, the back-up is able to take over the tasks if these are not finalized or achieved, thereby closing of the customer requests without impacting the customer negatively. Controls and checks have been integrated within the process in order to avoid such an incident from occurring again in the future*".

DECISION

On the basis of the foregoing the Commissioner considers that [redacted] did not have adequate procedures in place to deal with subject access requests, resulting with the complainant actually deprived of her right to access her data within the timeframe stipulated within the Regulation. Consequently, **the data controller is found to be in violation of Article 15 of the GDPR.**

After having taken into consideration:

- the controller's degree of cooperation with this Office;
- that the controller took immediate action to comply with the complainant's request as soon as the error in the security settings of the mail box used to communicate with the complainant was discovered;
- that the controller has now in place a better procedure introducing measures to improve the process to deal with the customers' requests to exercise their rights under the GDPR and to keep within the legal timeframes;

and also giving due regard to the circumstances contemplated under Article 83.2 of the GDPR and taking into account Article 83.1, [redacted] is hereby being served with an administrative fine of eight thousand euros (€ 8,000).

The administrative fine shall be paid to the Commissioner within twenty-five (25) days from receipt of this decision.

In addition, [redacted] is hereby being instructed to implement the appropriate technical measures to further enhance the measures already in place.

A copy of this decision is also being sent to the Polish Office for Personal Data Protection.

[redacted]

Saviour Cachia
Information and Data Protection Commissioner

Today, the 28th day of October, 2019