CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

The President

[redacted]

Examination of the case:
[redacted]

Paris, on 25 FEV. 2020

N/Réf.: MLD/JLI/KKR/XD/EMT/CM192961
(to be recalled in any future correspondence)

Dear Mr [redacted]

I am writing to you further to the exchanges of emails between the CNIL and your company's Data Protection Officer (hereinafter referred to as "DPO") in the context of the investigation of six complaints relating to problems encountered by users of [redacted] website in exercising their rights as provided for by the General Data Protection Regulation (GDPR).

I should remind you that the six complaints bear on difficulties encountered during exercise of the right to object and rights of access and portability.

The elements resulting from these exchanges lead me, in agreement with the other data protection authorities concerned by the management processing of your platform's users, **to issue reprimands to [redacted] regarding its obligations, in accordance with the provisions of Article 58.2.b) of the General Data Protection Regulation (GDPR).**

Indeed, the investigation of the complaints has pointed out, on the one hand, that a technical problem arised during summer 2018 had prevented the taking account of the communication preferences of some users and, on the other hand, that the [redacted]'s methods of responding to its users' access requests were not compliant with the provisions of the GDPR (1).

That being recalled, I take note that [redacted] has taken measures to improve the process for managing requests for the exercise of rights (2). I also note the fact [redacted] has given a satisfactory outcome to requests of each complainant.

1. Reminder of your obligations under the GDPR

➢ On the technical problem affecting objection to direct marketing

The CNIL asked your DPO to specify the extent of the consequences of the technical problem highlighted in the context of the complaint investigation, as well as the measures [redacted] has taken to remedy the said problem.

→ *On the technical problem's consequences*

Your DPO stated that "*during May 2018,* [redacted] *modified the presentation of product communication preferences with a view to enabling its users to give or withdraw their consent independently for each communication channel (email, SMS, and in-app messages or notifications) rather than there being a single choice for all channels.*

- *Such modification required (i) migration of communication choices previously made by users to communication categories redefined by* [redacted] *and (ii) synchronisation of such communication choices with [your] emailing tool so as to ensure that emails are only sent to users who have consented to receiving messages on [your part].*

However, an incident arose during migration, with the following consequences:

- *first of all, a mapping problem arose between the old and new consent management platform: where the old platform had assigned a "true" value to consents given and an empty value to consents not given/withdrawn, the new platform considered that empty values should be considered as "true" values (and not "false" as should have been the case);*

- *secondly, a synchronisation problem affected [your] emailing tool, preventing users' communication choices from being taken into account during communication campaigns".*

I note that your DPO specified that the incident had not only affected users who had made communication choices prior to migration to the new consent management platform (mapping problem), but also those who had modified their choices following such migration (synchronisation problem).

→ *On measures implemented in order to remedy the problem and restore users' communication choices*

Your DPO stated that [redacted] took the following measures:

- "*modification of the new migration script and application of the new script to all users registered before 25 May 2018;*
- *verification that users' communication choices had been included in our emailing tool, so as to make sure that users targeted by our campaigns had actually given their consent;*
- *campaigns during summer 2018 to inform users of the change in communication preferences and ask them to configure their choices accordingly".*

If I take note of the fact that the problem has been solved and that users' communication preferences have now been restored, the abovementioned facts lead me to remind you that **Article 24 of the GDPR** stipulates that "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure* [...] ***that processing is performed in accordance with this Regulation.***".

This being so, it is [redacted] responsibility to implement appropriate technical and organisational measures to ensure that its users' agreement or objection to receiving direct marketing are complied with.

Yet the facts outlined above show that [redacted] failed to fulfil its obligations as provided for by the GDPR, when, prior to migration of its consent management tool, it did not implement the necessary measures to take permanent account of and integrate its users' choices.

➢ **On methods of responding to right of access**

Your DPO stated that when [redacted] received an access request to his/her personal data from a user, such request was followed up in accordance with the following procedure:

- creation of a folder dedicated to the user on an SFTP server belonging to [redacted],
- deposit into the folder of a file containing all data on the user in [redacted]'s possession,
- communication to the user of usernames enabling him or her to connect to the dedicated folder.

Your DPO stated that connection username and password were communicated to the user by a message sent set to his/her [redacted] personal space or, in the absence of a [redacted] account, by email to the address used to access the service.

In this respect, I should remind you that personal data must be used in such a way as to guarantee its security, in particular by ensuring that appropriate technical and organisational measures are taken (Article 5.1 (f) of the GDPR). The Data Controller must implement measures that guarantee the confidentiality, integrity and availability of data processed (Article 32 of the GDPR).

Yet, failing prior authentication, common communication of username and password for connection to content containing personal data via one and the same channel does not seem appropriate in view of these provisions, if data security is to be guaranteed.

It is the Data Controller's duty to communicate connection username and password via two different communication channels. In this particular case, if the link to the SFTP server and the connection username can be communicated to the person concerned by email, the password must be sent to him/her via another channel (for example, by asking the person to receive it by SMS, orally, by telephone, or by post).

On this point, it is your responsibility to modify your procedure for making data available in the context of requests for right of access, so as to ensure that it is in compliance with the GDPR.

2. Measures taken by [redacted]

Finally, the exchanges between the CNIL and your DPO made it clear that [redacted] has implemented procedures designed to better manage inflows of requests from data subjects regarding their rights guaranteed by the GDPR.

In this respect, your DPO stated that [redacted]'s customer service received an average of 10,000 customer requests a week, sometimes peaking at over 12,000 requests, and that about 10% of such requests related to users' personal data (access, portability, modification and deletion).

This being so, I note that [redacted] has implemented a special procedure for managing requests concerning its users' data, at the address "[redacted]". The requests received via this address are sent to [redacted]'s customer service and are the subject of intervention tickets in order to guarantee their follow-up and traceability.

Finally, I take note of the fact that [redacted] is also implementing one-off measures designed to improve its customer service's responses to users exercising their rights as provided for by the GDPR.

[redacted]O has told the CNIL that a GDPR workshop for customer support teams has been held in [redacted] designed to raise their awareness on the data protection question, train them in the procedure for responding to customers' requests, and identify avenues for improvement.

I would ask you to continue with these initiatives and must advise you that, in the event of any further complaints, the CNIL reserves the right to make full use of the powers vested in it by the GDPR

Yours Sincerely,

[redacted]

This decision may be appealed before the French State Council within a period of two months following its notification.