CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

The Chair

[redacted]

Paris, 06 JAN. 2021

Our ref.: MLD/PVT/SGE/RAL201023
Case submission nos 20006815, 20010739 and 20011014
(please quote in all correspondence)

Dear Madam,

I am writing further to the exchanges between your Data Protection Officer (DPO) and the CNIL, in the context of examining three complaints that were forwarded to us by the Irish Data Protection Commission pursuant to Article 56.1 of the General Data Protection Regulation (GDPR).

These complaints concern [redacted] sending of an email to its customers without their email addresses being placed in blind carbon copy (BCC). In an email dated 18 September of this year, your DPO explained that "*the number of email addresses concerned amounted to 37, some of which were generic email addresses associated with legal entities*".

Moreover, it has been specified that this incident is due to a human error committed by your service provider [redacted] in the context of using an IT tool for sending "*emails to all of the people of a flight*".

First, I would remind you that, as data controller, it is your responsibility to ensure the security and privacy of the personal data you process, including through your processors, by implementing appropriate technical and organisational measures (Article 32, GDPR).

On that note, provision must be made for measures that are aimed at preventing an email being sent to a group of individuals without the recipients' email addresses being placed in the "BCC" field to ensure they are invisible, including when a processor sends such emails.

Second, I would point out that such actions amount to a personal data breach under Article 4.12 of the GDPR, but that no personal data breach has been notified to the CNIL in this regard.

Now, the provisions of Article 33 of the GDPR provide that "*In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay*".

Although your DPO has explained that, in light of the low volume of personal data concerned by said breach, [redacted] did not consider it necessary to communicate the breach to the data subjects as stipulated in Article 34 of the GDPR, the breach in question does seem likely to generate a risk – even a moderate one – for the data subjects. As such, [redacted] failed to comply with its obligation to notify such a breach to the CNIL.

I note that, since this incident, "*a reminder of the procedure*" has been issued to "*all of* [your] *service provider's staff*" to ensure it does not happen again. However, all of these facts prompt me, in agreement with the other European data protection authorities concerned by the processing, to **remind [redacted] of its obligations regarding the aforementioned points, in accordance with the provisions of Article 58.2.b) of the General Data Protection Regulation (GDPR).**

The requirements reiterated above must be fulfilled without fail in the future. Where necessary, the CNIL will conduct subsequent verifications and reserves the right to apply the whole panoply of powers conferred upon it by the GDPR and the French Data Protection Act (Act of 6 January 1978 amended).

My staff ([redacted]@cnil.fr) is at your disposal for any further information.

Yours sincerely,

[redacted]

This decision may be appealed before the French Conseil d'Etat within two months of its notification.

NB: Copy to [redacted] Data Protection Officer at [redacted]