

ARTICLE

COMMERCIAL PROSPECTING AND RIGHTS OF INDIVIDUALS: €600,000 FINE IMPOSED ON GROUPE CANAL+

Intellectual Property, Media, and Art Law | 24/10/23 |

On October 12th, French data protection authority CNIL imposed an administrative fine of €600,000 on GROUPE CANAL+ (equivalent to 0.03% of the company's 2022 revenue).

WHAT BREACHES WERE IDENTIFIED?

Failure to obtain the consent of the individuals concerned for the implementation of commercial prospecting by electronic means (Articles L. 34-5 of the French Post and Electronic Communications Code and Article 7 of the General Data Protection Regulation (GDPR)).

- As already indicated by the CNIL in its practical information sheet on the transmission of data to partners for direct marketing purposes, if the organization sharing data chooses to obtain consent from individuals for direct marketing conducted by its partners, **then these partners must be exhaustively listed** at the time of consent collection to ensure that it is informed and valid. Merely stating that data will be shared with "partners", without providing further details, does not suffice.
- Even if the direct marketing activities are carried out by a processor who directly receives the email addresses of the individuals canvassed, it is still **the identity of the direct marketing organization on whose behalf of the processor acts that must be included in the list of partners with whom the data is shared.**

Failure to inform the individuals concerned of the processing of their personal data (Articles 13 and 14 of the GDPR)

- The CNIL reiterated, as it had previously done in its SAN-2020-008 decision of November 18th, 2020 concerning CA RREFOUR FRANCE, that a privacy policy **must specify precise and non-generic data retention periods**. Merely indicating that data is stored for as long as legally required and then archived for the length of the statute of limitations is too vague.
- The rapporteur criticized the lack of information in the privacy policy regarding the possibility for individuals to file a complaint with the CNIL (breach of Article 13 of the GDPR). However, the CNIL's restricted committee found that this information was in fact available even if it was not easily accessible (breach of Article 12 of the GDPR). **Nevertheless, since the rapporteur did not characterize this violation in her report, the CNIL concluded that it could not use it as a basis for sanctioning the company.**
- Regarding telephone canvassing, the CNIL reiterates, as it had done in its SAN-2022-011 decision of June 23rd, 2022 concerning TOTALENERGIES ELECTRICITÉ ET GAZ France, that the information provided orally to individuals canvassed by phone may be limited to the most important elements (including, even though the CNIL does not mention it here: the fact that the call is being recording, the purpose pursued, and the possibility to object) provided that a means for receiving more comprehensive information is indicated (such as a keypad option on the phone, an email sent to the individual, or a reference to a web page).

Breaches of obligations concerning the exercise of individuals' rights (Articles 12 and 15 of the GDPR):

- The CNIL reiterated the importance of handling requests within the specified time limits and decided to fine the company on this basis, even though it clarified that this breach was not a systemic failure to provide information on the exercise of rights.
- The CNIL also decided to fine the company for improperly categorizing a received request (the company had considered that the request aimed to obtain proof of a subscription contract and thus fell outside the scope of the GDPR, while the CNIL considered it to be a request for access and erasure, which should therefore have been handled as per the time limits and procedures mandated by the GDPR).





Failure to provide a contractual framework (contract or other legal act) for processing carried out on behalf of a controller (Article 28.3 of the GDPR)

- The CNIL insisted, as it had in its SAN-2023-003 decision of March 16th, 2023 concerning CITYSCOOT, on the importance of ensuring that contracts with processors effectively include all of the information required by Article 28 of the GDPR.

Failure to ensure the security of personal data (Article 32 of the GDPR)

- In terms of authentication, the CNIL emphasized the need to ensure that a password used by employees to authenticate on software remains confidential. However, the CNIL determined that storing such passwords in a hashed form using the MD4 algorithm was not in line with state-of-the-art practices, as previously indicated in recommendations by the CNIL and the national cybersecurity agency ANSSI. The CNIL also considers that implementing additional security measures cannot remedy or compensate for the use of an inherently weak hashing algorithm such as MD4.

Failure to notify the CNIL of a personal data breach (Article 33 of the GDPR)

- Following an update to the CANAL+ customer portal, subscribers were able to view information about other subscribers (10,154 individuals). However, the company did not notify the CNIL of the data breach. The CNIL opined that the company should have notified this breach, given that (i) subscriber postal addresses and phone numbers were disclosed, which has the potential to *"infringe upon subscribers' right to privacy,"* and (ii) the number of affected individuals is *"not negligible."*
-