DATA-SCRAPING: A CLEAR LIMITATION BY THE FRENCH DATA PROTECTION AUTHORITY ON DIRECT MARKETING PRACTICES USING DATA FROM THIRD PARTY SERVICES

Date: 10 March 2021

French Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Alexia Montagnon, Clara Schmit

The French Supervisory Authority (CNIL) wrapped up 2020 with a EUR 20,000 fine against NESTOR, a French food preparation and delivery company catering to office employees (see full decision here in French).[1]

The CNIL highlighted various breaches of the General Data Protection Regulation (GDPR)[2] and the ePrivacy Directive regarding the processing of prospects and clients' personal data by the CNIL, most notably:

- The lack of prior consent of the prospects to receiving direct marketing communication by electronic means, thereby violating Article L.34-5 of the French Post and Electronic Communications Code (CPCE);[3]
- The failure to properly inform individuals[4] whether:
  - Upon the creation of their account on the company's platform, or
  - Upon indirect collection through external sources;
- The failure to properly address Data Subjects' Access Requests (DSAR).[5]

While the fine is rather limited in view of the maximum potential amount of EUR 20 million or four percent of the turnover (whichever the greater), this decision presents an opportunity to examine web scraping and direct marketing practices, which are rapidly developing.

DATA SCRAPING AND DATA PROTECTION RULES

NESTOR built a database of prospective clients by automatically collecting personal data made publicly available through third party platforms, a practice known as “data scraping” or “web-scraping”, widely used by startup and emerging companies to quickly develop their marketing campaigns.

This database, comprising 635,033 contacts, was created and utilized with the assistance of third party services:

- The personal data was initially collected through LinkedIn's “Sales Navigator” functionality, which can identify individuals working in a company within a given region;
- A second company then added the professional e-mail addresses of the individuals; and
- A third company proceeded with the dispatch of prospecting e-mails on behalf of NESTOR.

Under Article 13.1 of ePrivacy Directive, such practice would require a GDPR-compliant[6] consent by the data subject prior to sending direct marketing communication through electronic means. Indeed, the ePrivacy Directive prohibits direct marketing via “electronic means” (i.e. emails, text messages, facsimile or automated calling machines[7]), unless such marketing practices are undertaken by the entity which effectively directly collected the personal data in the first place, within the framework of a sale of a product or the provision of a service, and aim to offer similar products and services.

This Article of the ePrivacy Directive was subsequently implemented under French law in the Article L.34-5 CPCE.

Since NESTOR did not collect the personal data not from the individuals itself but through LinkedIn's functionality, CNIL concluded that prior consent was required.

In addition, companies relying on indirectly collected personal data also fall within the scope of Article 14 GDPR, which mandates the provision of certain information to data subjects, at least within 30 days from the provision (or harvesting) of their personal data.

NESTOR'S CASE: THE SPECIFICS OF THE LEGAL BASIS

While the ePrivacy Directive has been implemented differently in various EU Member states (and while waiting for its successor, the ePrivacy Regulation, to harmonize this area), the CNIL interpretation may have EU-wide consequences for all companies.

Most notably, certain EU Member states elected to implement the ePrivacy Directive with a strict interpretation, i.e. consent requirement for all data subject recipients. Other included a consent exemption for B2B direct marketing. In that regard, France's exemption takes the form of a single webpage (non-binding and able to be amended at any time) on a company's website stating that prior information and a right of opposition offered to professionals is sufficient for direct marketing purposes.

NESTOR built its defense on that exemption, arguing it did not require any prior consent and could instead rely on its legitimate interest as a legal basis for the direct marketing operations through electronic means.

However, the CNIL rejected that argument on the basis that messages regarding food delivery in the workplace had little connection with the prospects' effective professional activity, despite such food services being performed during prospect's professional activity. According to the CNIL, a direct link between the marketing operation and the prospects' professional activity was necessary to justify relying on legitimate interest.

Additional aggravating factors consisted in the lack of information provided to the individuals about the data processing operations and the lack of opportunity to oppose such collection.

The CNIL decision has been published six months after the CNIL released its position on the collection of publicly available personal data (see our previous alert here) and is a stark reminder that the mere availability of data online would not, in and of itself, justify their collection and re-use without proper diligence. Moreover, aside from data protection concerns, data scraping may also be subject to additional restrictions, such as intellectual property or database protection.

WHY THIS DECISION MATTERS?

This decision might seem anecdotal given the immaterial fine. Nevertheless, its significance is not simply based on its fine's low amount but rather on the subject matter of the decision itself. The decision is a firm limitation by the CNIL to the practice of web scraping via third party platform, such as LinkedIn, for direct marketing purposes, and a potential indication that the current B2B exemption may come to an end, at least under its current scope.

To give greater significance to this case, the CNIL made the decision public, and provided a very comprehensive article of this decision on its website, detailing the various breaches committed by the company.

This significance is also highlighted by the decision published by the CNIL the previous day, on 7 December 2020, against PERFORMECLIC[8] which also addressed direct marketing and indirect collection (however not related to data scraping). This seems to indicate that further investigations on direct marketing practices are a priority for the French Supervisory Authority for 2021.

The K&L Gates Data Protection team remains available to assist you in achieving compliance of your direct marketing activities across Europe.

FOOTNOTES

[1] CNIL, Decision SAN-2020-018, 8 December 2020 (in French).

[2] Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 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).

[3] Article L.34-5 of the French Post and Electronic Communications Code (in French).

[4] Article 12 and 13 GDPR.

[5] Article 15 GPDR.

[6] As pointed out in the European Data Protection Board (EDPB)'s opinion on the interplay between the ePrivacy Directive and the GDPR, when consent is required under the ePrivacy Directive, consent would necessarily be required as the legal basis under GDPR.

[7] It does not, however, restrict postal marketing or direct phone call with human operators.

[8] CNIL, Decision SAN-2020-016, 7 December 2020 (in French).

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM