May 2020

The position of the CNIL on Data Privacy implications of Web scraping

On April 30, 2020, the French data protection authority ("DPA", known as the CNIL) published guidance concerning the practice of scraping publicly available website data to obtain individuals' contact information for purposes of selling such data to third parties for direct marketing purposes. The guidance was issued following inspections carried out by the CNIL in 2019.

Importantly, the guidance states that even if contact information is scraped from publicly accessible websites, the individuals who posted the information did not reasonably expect to have it scraped for prospecting, and as such, the contact information is still **personal data** under the GDPR and cannot be re-used for marketing without the consent of the data subject.

The guidance emphasizes that such consent should be obtained prior to any reuse of the data for marketing purposes and must be **freely given, specific, informed and unambiguous**. According to the CNIL, the acceptance of general T&C's mentioning that the individual accepts to receive marketing communications is insufficient, as it is not specific. In addition, the CNIL points out that the individuals' rights under the GDPR must also be complied with, such as the right for an individual to oppose the processing of their data.

The guidance goes on to proffer the CNIL's recommendations as to additional steps that should be taken before using web scraping tools:

- Verify the nature and origin of the data that will be scraped: the guidance notes that some tools extract information from websites whose terms of use prohibit the extraction and re-use of data for marketing purposes. In this case, the CNIL emphasizes that the practice is unauthorized.
- Minimize data collection: companies using web scraping tools must avoid collecting irrelevant and excessive information, particularly if that information is sensitive (e.g., data concerning health, religion or sexual orientation of individuals).
- Provide notice to individuals: companies using web scraping tools must provide notice to individuals whose data has been extracted for direct marketing, at the latest at the time of the first communication with those individuals. The notice must contain all the information listed in Article 14 of the GDPR, including the source of the data.
- Manage the contractual relationship with the web scraping service provider: when companies engage a web scraping service provider, they must ensure that the above measures will be complied with by the service provider. In addition, companies must ensure that they have a proper data processing agreement in place with that service provider in compliance with Article 28 of the GDPR.

- Carry out a Data Protection Impact Assessment ("DPIA") if necessary: if the GDPR article 35 criteria are met, a DPIA must be carried out before implementing the data processing. Even if a DPIA is not required, the Guidance emphasizes that it is best practice to carry one out.

This is not the first time that a European DPA has investigated data scraping activities. In March 2020, the Polish DPA issued its first fine under the GDPR against Bisnode, a Swedish-headquartered company that obtained personal data from public databases and registers in order to provide verification services and reports. The personal data focused on current and past entrepreneurs and business owners. In order to comply with the GDPR article 14 obligation to explain to individuals how they process the personal data, Bisnode had sent emails to affected individuals with known addresses and posted notices on its website, but it did not send postal notification to millions of other individuals or entities due to the administrative cost and burden of doing so. Although GDPR article 14(5) releases data controllers from their obligation to inform affected individuals where "the provision of such information proves impossible or would involve a disproportionate effort" or where the obligation "is likely to render impossible or seriously impair the achievement of the objectives of that processing", the Polish DPA surprisingly deemed that postal notification was not impossible and therefore issued a fine for such a violation.

* *