

FRENCH DATA PROTECTION AUTHORITY RELEASES POSITION ON THE COLLECTION OF PUBLICLY AVAILABLE PERSONAL DATA

Date: 26 May 2020

European Privacy and Data Protection Alert

By: Claude-Étienne Armingaud, Clara Schmit, Emmanuel Gautier-Nguyen

While privacy concerns associated to the implementation of COVID-19 contact tracing apps across the European Union exist, the French Data Protection Authority (CNIL) also released a position paper on the collection of publicly available personal data for the purpose of direct marketing on 30 April 2020 and following numerous individual complaints.

Such complaints notably related to companies automating the collection of telephone and email contact information from individuals, appearing on consumer-to-consumer (C2C) websites (e.g. real estate ads) or from online directories, a practice known as “web scraping”.

Among all investigations carried out by the CNIL, not a single web scraping activities complied with the General Data Protection Regulation ([GDPR](#)) and the [French Data Protection Act](#) no. 78-17 dated 6 January 1978. In particular, the CNIL identified the following discrepancies:

- A lack of information of the individuals, in particular information related to the source of collection of personal data, as mandated by [Article 14 GDPR](#);
- A lack of prior explicit consent of individuals before being solicited by electronic messages or automatic calling machines acting on behalf of companies to promote their products or services, outside of the exceptions listed under Article 13 of the Directive 2002/58/EC dated 12 July 2002 ([ePrivacy Directive](#)); and
- Failure to comply with the individuals' right to object/opt-out under [Article 21 GDPR](#).

The main discrepancy lies in the fact that individuals initially provided their personal data to a specific data controller for specific purposes. While re-use by another data controller is not prohibited per se, it is however subject to specific requirements, and mainly prior consent when such re-use relate to direct marketing activities for products or services which are neither similar to those of the initial data controller nor provided directly by it.

WHAT SHOULD COMPANIES DO WHEN USING WEB SCRAPING?

When using web scraping software to collect personal data publicly available on the internet, companies should focus primarily on (i) the effective and complete information of individuals on the processing operations and (ii) the collection of their prior consent for use of their data for direct marketing purposes by electronic means.

As regards the nature of such consent, the CNIL has not issued any specific framework - the general requirements for consent therefore apply, i.e. (i) freely given, (ii) by an affirmative act (iii) specific, (iv) informed and (v) unambiguous.

Consequently, the mere acceptance of terms of use or a privacy policy, either explicitly or by continued browsing, on a given website would not be construed as a valid consent for web scraping operations implemented by a third party.

In addition, the information requirement for a valid consent would mandate that all disclosure pertaining to the indirect collection of personal data under [Article 14 GDPR](#) be provided at the time the consent is obtained. While consent may not be required for other purposes than direct marketing through electronic means, such information requirement will still need to be complied with regardless of the purposes at the earliest occurrence between:

- Thirty days further to the indirect collection of the personal data through web scraping;
- The first communication with the individual initiated further to the web scraping; or
- Further disclosure of the personal data to another entity, downstream from the entity which undertook the web scraping.

This position was also an opportunity for the CNIL to remind that web scraping activities must comply with all data protection rules laid down not only by GDPR and the French Data Protection, but also other legal framework such as database protection. This position also builds on the enforcement of GDPR across the European Union and most notably, the [first fine](#) published by the Polish Data Protection Authority (UODO) in 2019 against a company which processed the personal data obtained from publicly available sources, inter alia from the Central Electronic Register and Information on Economic Activity, and processed the data for commercial purposes. The initial fine corresponded to EUR 220,000 but was lowered upon [appeal](#), while the rationale for the fine was upheld.

This will thus require from companies involved in web scraping to:

- Verify the nature and the origin of personal data extracted from the internet. Most of terms of use explicitly state that extraction and reuse of personal data publicly accessible on their services is not allowed. In this case, and provided that the initial publisher is deemed the “maker of the database” under [Directive 96/9 dated 11 March 1996](#), such extraction is prohibited;
- Ensure that the contact information collected are not already included in Do-Not-Call/Do-Not-Contact lists, e.g. [BLOCTEL](#), [Signal Spam](#), [33700](#) in France;
- Minimize data collection and not indiscriminately extract all data available on the third party website;
- Ensure that any of their processors involved in the web scraping operations on their behalf comply with the above, through data protection agreements mandated under [Article 28 GDPR](#), by specifying the main characteristics of the data processing operation and obligations of the parties;
- Conduct a data protection impact assessment (DPIA) if required by Article 35 GDPR. Even if it would seem that the intrinsic sensitivity of web scraping may not initially require appears that such assessment is not required, the CNIL highlighted that such assessment is one of the main tool to verify that data processing is indeed compliant. Consequently, it may become good practice to conduct a preliminary DPIA, in order to document and justify why a full-fledged DPIA is not required.

KEY CONTACTS



CLAUDE-ÉTIENNE ARMINGAUD
PARTNER
PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM



CLARA SCHMIT
ASSOCIATE
PARIS
+33.(0)1.58.44.15.11
CLARA.SCHMIT@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.