FRENCH SUPERVISORY AUTHORITY PUBLISHES GUIDANCE ON THE USE OF WEBSITE ANALYTICS IN COMPLIANCE WITH GDPR REQUIREMENTS

Date: 21 June 2022

Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Camille J. Scarparo

Following the 2020 Court of Justice of the European Union's (CJEU) ruling invalidating the Privacy Shield (see our alert here), personal data transfers from the European Union to the United States required EU companies to implement additional safeguard mechanisms, as the CJEU considered that U.S. legislation did not provide sufficient guarantees against the risk of access by public authorities (including intelligence services) to the imported data.

Further to this ruling, several EU Supervisory Authorities (SA) received complaints from None of Your Business (NOYB), Max Schrems' association, relating to the use of U.S.-based website analytics solutions used to measure online audience (Analytics Service Solutions) by EU data controllers. In February 2022, following the position adopted by the Austrian SA in December 2021 (see an online anonymized version here—German language only), the French Data Protection Authority (CNIL) sent more than a hundred formal notices to EU data controllers (see an online anonymized version here—French language only) on the grounds that the use of Analytics Service Solutions led to insufficiently regulated transfers to the United States. These notices raised the question whether further to the provisions of Chapter V of the GDPR, technical measures or settings could allow for the compliant use of Analytics Service Solutions.
In its 7 June 2022 communication, the CNIL considered several measures as insufficient, such as:

- Merely implementing the base version of the European Commission's Standard Contractual Clauses;
- Simply changing the settings for the processing of IP addresses;
- Using encryption of the identifier generated by Analytics Service Solutions; or
- Replacing such identifier with an identifier generated by the website operator, as such measure provides little or no additional guarantee against the possible reidentification of data subjects.

The main issue encountered when using Analytics Service Solutions was considered to be the direct contact, through an HTTPS connection, between the individual's terminal and servers managed by the Analytics Service Solutions provider, allowing servers to collect the users' IP address.

However, according to the CNIL, severing the link between the terminal and the server could solve this issue and reconcile the use of Analytics Service Solutions with GDPR requirements.
In order to do so, the CNIL established that using a proxy server to avoid any direct contact between the internet user's terminal and the servers of the Analytics Service Solution could be contemplated as a solution.

Nevertheless, additional measures should still be implemented, such as pseudonymization prior to the export of the personal data (c.f. European Data Protection Board's Recommendations 01/2020 of 18 June 2021). Data controllers should however be able to demonstrate that the pseudonymized personal data cannot be attributed to an identified or identifiable natural person, even if (i) cross-checked with other information and (ii) taking into account the considerable means available to the public authorities likely to proceed with such reidentification.

In addition, the CNIL requires for several measures to be implemented for the “proxyfication” to be valid and limit the transferred data, including but not limited to the following:

- The absence of transfer of the IP address to the servers of the Analytics Service Solution. If a location is transmitted to the servers of the Analytics Service Solution, it must be carried out by the proxy server itself, and the level of precision must ensure that this information does not allow the person to be reidentified (e.g., by using a geographical mesh ensuring a minimum number of internet users per cell).
- The replacement of the user identifier by the proxyfication server. To ensure effective pseudonymization, the algorithm performing the replacement should ensure a sufficient level of collision (e.g., a sufficient probability that two different identifiers will give an identical result after hashing) and include a variable temporal component (adding a value to the hashed data that evolves over time so that the result of the hashing is not always the same for the same identifier).
- The removal of referrer information external to the website.
- The removal of any parameter contained in the collected URLs (e.g., the Urchin Tracking Modules but also the URL parameters allowing internal routing of the website).
- The reprocessing of information that can participate in the generation of a fingerprint, such as user-agents, to eliminate the rarest configurations that can lead to reidentification.
- The absence of any collection of identifiers between websites (cross-website) or deterministic (e.g., CRM, unique ID).
- The removal of any other data that could lead to reidentification.

Furthermore, hosting conditions must be taken into account with regard to the proxyfication server. It should be hosted under conditions which would guarantee that the personal data processed will not be transferred outside of the European Economic Area (EEA) to a country that does not ensure a level of protection essentially equivalent to the one provided for in the EEA without sufficient technical and organizational measures as required by the Schrems II ruling. To provide additional guidance to this communication, the CNIL published on 7 June 2022 an online Q&A stating that following such recommendations, the notified companies have a period of one month to bring their Analytics Service Solutions' international transfers into compliance. This one-month period may be renewed at the explicit request of the companies using such solutions.

In any case, as implementing the aforementioned measures can be costly and complex, data controllers also have the possibility to opt for the use of Analytics Service Solutions that do not transfer personal data outside of the European Union.

K&L Gates Global Data Protection team (including in each of our European offices) remains available to assist you in achieving the compliance of your data transfers at global level.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

CAMILLE J. SCARPARO
ASSOCIATE

PARIS
+33.1.58.44.15.11
CAMILLE.SCARPARO@KLGATES.COM

