Brève
23 mai 2022

Google Analytics jugé de nouveau contraire au RGPD par l'autorité de protection des données autrichienne

Dans une décision du 22 avril 2022, l'autorité de protection des données autrichienne s'est de nouveau prononcée sur la question de la licéité du recours à Google Analytics dans le cadre de transfert de données à caractère personnel.

Dans la lignée de sa décision de décembre 2021, l'autorité a considéré que l'usage de Google Analytics par un responsable de traitement est contraire à l'article 44 du Règlement Général sur la Protection des Données (ci-après, « RGPD »). Ledit responsable de traitement et Google étaient tous deux mis en cause.

Pour mémoire, cet article pose le principe général selon lequel *« Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis ».* C'est cet article qui annonce qu'un transfert de données d'européens hors Union Européenne ne peut se faire que (i) vers un pays de législation adéquat ou (ii) moyennant une des garanties ou exceptions prévues par les articles suivants du RGPD.

Pour sa défense, Google soulignait dans un premier temps que des clauses contractuelles types avaient été conclues afin d'encadrer le transfert de données à caractère personnel. En outre, des mesures supplémentaires telles que l'anonymisation des adresses IP avaient été mises en œuvre pour garantir un niveau de protection des données à caractère personnel adéquat.

En réponse, l'autorité s'est fondée, désormais classiquement, sur la décision « *Schrems II* » du 16 juillet 2020 rendue par la Cour de Justice de l'Union européenne (ci-après, « CJUE ») ayant invalidé la décision d'adéquation « *Privacy Shield* ». La CJUE avait alors jugé que la législation américaine n'apportait pas de garanties équivalentes au RGPD et devait donc être considérée comme non adéquate avec la protection des données à caractère personnel offerte par le RGPD.

En effet, Google est considéré comme un fournisseur de services de communications électroniques au sens du 50 U.S. Code § 1881(b) (4) et, en tant que tel, est soumis à la surveillance des services de renseignement américains en vertu notamment de la section 702 du FISA. Les autorités américaines sont donc en mesure, fût-ce seulement en théorie, d'obtenir de Google l'accès aux données de son client, où que celles-ci soient stockées.

Dès lors, la mise en place de mesures supplémentaires aux clauses contractuelles types telles que l'anonymisation des adresses IP par Google n'est pas suffisante aux yeux de l'autorité autrichienne, qui a estimé que les possibilités de surveillance et d'accès par les services de renseignement américains perduraient.

Plus précisément, l'autorité autrichienne explique avoir rejeté l'argumentaire de Google fondé sur l'anonymisation des adresses IP pour deux raisons.

D'une part, l'anonymisation ne concernait que les adresses IP en tant que telles : les données telles que les identifiants en ligne, les cookies ou les données des appareils étaient transférées en clair.

D'autre part, l'anonymisation n'avait lieu qu'après le transfert des données à Google : le processus d'anonymisation étant en soi un traitement de données à caractère personnel, Google avait en sa possession les données en clair, peu important l'anonymisation ultérieure.

Dans un second temps, Google prétextait avoir effectué une *approche par les risques* pour justifier les transferts de données à caractère personnel. L'entreprise arguait que le risque d'accès par les services de surveillance américains était faible en l'espèce, essayant de démontrer par-là que ses mesures additionnelles étaient efficaces et suffisantes, afin de valider le transfert de données.

Selon Google, l'approche par les risques ressortirait clairement de la décision « *Schrems II* », de la Foire Aux Questions (FAQ) « *Schrems II* » mise en ligne par le Comité Européen de la Protection des Données (ci-après, « CEPD ») ainsi que des recommandations 01/2020 de ce dernier.

De surcroît, Google affirmait que l'approche par les risques est prévue par le RGPD lui-même dans certaines de ses dispositions, ce que ne remet d'ailleurs pas en cause l'autorité autrichienne (Art. 24(1) et (2), Art. 25(1), Art. 30(5), Art. 32(1) et (2), Art. 34, paragraphe 1, art. 35, paragraphes 1 et 3, ou l'art. 37(1) (b) et (c) du RGPD précise l'autorité).

Cependant, ce nouvel argument développé par Google (qui n'est pas propre à Google, un grand nombre de prestataires américains, dont les grands cloud providers, et leurs clients européens ayant adopté la même approche), a également été rejeté par l'autorité autrichienne.

Cette dernière a d'abord considéré que dès lors que le RGPD prévoit expressément les cas de recours à l'approche par les risques à certains de ces articles, et, qu'à l'inverse, l'article 44 du RGPD ne prévoit pas la possibilité de se fonder sur celle-ci, les responsables de traitement et sous-traitants ne peuvent y avoir recours pour justifier un transfert de données ou prétendre que les mesures additionnelles mises en place seraient « efficaces ».

Il en résulte qu'il n'est pas possible de faire une application analogue de l'approche par les risques à l'article 44 du RGPD, ce qui serait contraire à l'intention du législateur selon l'autorité autrichienne. Autrement dit, l'approche probabiliste est repoussée : il n'est pas pertinent de considérer qu'un accès par les autorités étrangères est « peu probable » : du moment qu'il reste possible, le transfert est illicite en l'absence de mesures additionnelles réellement efficaces.

L'autorité autrichienne a ensuite jugé que si la CJUE, dans son arrêt « *Schrems II* », impose aux responsables de traitement et sous-traitants exportateurs « *l'évaluation du niveau de protection* » des données dans le pays tiers, cette évaluation ne doit pas être confondue avec l'approche par les risques qu'a effectué Google.

En effet, la CJUE a précisé dans sa décision que « *l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées* » et que le pays tiers garantisse aux personnes concernées des « *droits opposables et voies de droit effectives* ».

Selon l'autorité autrichienne, « *l'évaluation du niveau de protection* » du pays tiers diffère donc de l'approche par les risques en ce que cette dernière nécessite de vérifier le caractère sensible ou non des données à caractère personnel transférées.

Au passage, l'autorité autrichienne écarte rapidement l'argument de Google selon lequel l'interdiction de ses traitements aurait des conséquences économiques sur les entreprises européennes : l'autorité de contrôle n'a pas pour rôle de statuer en opportunité à partir de considérations économiques, mais d'interpréter la réglementation et de préciser ce qui peut être considéré comme une mesure efficace, et ce qui ne l'est pas.

Enfin, l'autorité écarte également l'argument selon lequel les recommandations 01/2020 du CEPD justifieraient le recours à l'approche par les risques en jugeant que les recommandations indiquent seulement qu'il est nécessaire de vérifier si les lois problématiques du pays tiers s'appliquent à chaque transfert de données et non qu'il est nécessaire de vérifier le caractère sensible ou non des données à caractère personnel transférées.

En conséquence, selon l'autorité autrichienne, l'approche par les risques doit être exclue en matière de transferts de données à caractère personnel et le recours à l'outil à Google Analytics reste contraire au RGPD. Cette décision prend à rebours le positionnement de très nombreux commentateurs de la décision « *Schrems II* » et des recommandations du RGPD, et livre une lecture stricte des articles du RGPD.

Cette décision s'inscrit en outre dans le fil des précédentes décisions des autorités européennes (CNIL, 10 février 2022, mise en demeure d'un gestionnaire de site web pour l'utilisation de Google Analytics), et autorité de contrôle de Bavière (BayLDA, 15 mars 2021, LDA-1085.1-12159/20-IDV), qui avaient déjà considéré que les mesures avancées par Google relatives à sa volonté de « challenger » les demandes d'accès des autorités américaines pour vérifier leur licéité, d'informer le responsable de traitement de telles demandes si la loi US le permet, ou encore de publier des « rapports de transparence », ne constituent pas non plus des mesures « efficaces » permettent de mettre les données personnelles des européens absolument à l'abri de tout accès des autorités américaines.

La situation se crispe donc encore un peu plus, au grand dam des responsables de traitement français et européens qui recourent à des fournisseurs de technologies numériques américains. Si les autorités de contrôle européennes n'ont pas, à ce jour, prononcé de sanction forte contre ces utilisateurs, et si le Conseil d'Etat a quant à lui validé le recours à AWS dans l'affaire *Doctolib* (Conseil d'État, Juge des référés, 12 mars 2021, 450163), la lecture des décisions de ces autorités, à mesure que les assignations de l'association NOYB aboutissent, montrent que l'étau se resserre.

Si un nouveau *Privacy Shield* a été annoncé, l'accord sur son contenu est encore loin et dans cette attente, le transfert de données personnelles à des prestataires étrangers, non rattachés à des législations adéquates, continue de constituer une menace sérieuse sur la licéité des traitements effectués. Cette situation doit pousser les entreprises françaises à recourir le plus possible au chiffrement des données de bout en bout, au repos comme en transit, via des clés de chiffrement fournies et opérées par des prestataires qui ne sont pas soumis aux législations étrangères.

Contact : Thomas Beaugrand, Counsel
beaugrand@dsavocats.com