digital dpo

Infos Privacy Shield

Le nouveau Privacy Shield attendu dans les prochains jours

Devrait être publié par la Maison-Blanche la semaine du 3/10 (selon Politico).

Process à suivre : proposition Commission UE + avis EDPB + avis États Membres puis ratification Commission UE => devrait durer de 4 à 6 mois.

Contenu non connu à ce jour : mais il prévoirait un « mécanisme de recours indépendant à deux niveaux doté d'un pouvoir contraignant ».

Cependant le choix d'un Ordre Exécutif provoque des doutes :

- FISA est un texte législatif validé par le parlement
- Un Executive Order est révocable à tout moment par le Président des USA

Les Cnil européennes, l'activiste **Max Schrems**, le **directeur de l'Anssi, Guillaume Poupard**, et **plusieurs entreprises françaises** ont ainsi fait part de leurs doutes.

Source Contexte le 29/09/2021

digital dpo

Attention des CNILs sur les transferts

L'EDPB a initié son 1er **cadre d'application coordonné :** 22 autorités de contrôle lancent des investigations sur **l'utilisation, par le secteur public, de services utilisant le cloud.**

L'utilisation de l'informatique en nuage (*cloud*) est une des 3 priorités de la CNIL en 2022, dû à la présence ou la probabilité de transferts hors UE.

Le 21 septembre, la Cnil danoise s'ajoute au cortège contre Google Analytics le 21/09

« *Vous ne pouvez pas utiliser Google Analytics dans sa forme actuelle sans mettre en place des mesures supplémentaires* »

- Comme les CNILs autrichienne, française et italienne, elle considère qu'en l'état, Google Analytics ne protège pas efficacement les données.
- Elle recommande de **pseudonymiser les données en s'appuyant sur le guide de la CNIL française**. A défaut, d'arrêter d'utiliser Google Analytics.

- La Cnil a martelé le message en juin, recommandant fortement aux acteurs français d'agir pour éviter le transfert de ces données personnelles vers les États-Unis.

Actions de la CNIL

- Février 2022 — GA fait l'objet de 3 mises en demeures
- Juin 2022 — 2 publications de la CNIL
  - « Google Analytics et transferts de données : comment mettre son outil de mesure d'audience en conformité avec le RGPD ? »
  - Publication d'une FAQ « sur les mises en demeure de la CNIL concernant l'utilisation de Google Analytics »
- Juillet / Août 2022 — Saisines adressées aux éditeurs

digital dpo

Contenu des saisines

- Lettre envoyée aux DPO des éditeurs concernés.

- Signalement que la CNIL a vu dans les CMP ou dans les cookies déposés la présence de GA alors qu'elle en a déclaré l'utilisation en l'état « illégale »

- Les questions portent sur :
  - Les données collectées au travers de GA
  - Les destinataires des données collectées
  - L'existence de transferts de données vers les US selon l'éditeur du site
  - Les garanties contractuelles (CCT) signées
  - Les mesures de sécurité additionnelles apportées

- La CNIL accorde un délai d'un mois pour répondre

GT DPO : Suite données aux saisines

- 3 cas de figure se dégagent :
  1. les éditeurs qui n'avaient plus de tag GA à la date de réception du courrier
  2. les éditeurs qui peuvent migrer entièrement vers une autre solution et se passer de GA, moyennant l'octroi d'un délai supplémentaire par la CNIL
  3. les éditeurs dont l'architecture dépend entièrement de GA, et qui ne prévoient pas à court ou moyen terme de désactiver GA malgré la plainte

- Prochaines étapes :
  - 29 Septembre : Réunion avec la CNIL qui apportera des premiers éléments de réponse suite à notre demande de conseil informelle
  - 4 Octobre : réunion debrief de la réunion CNIL du 29 avec les DPO membres du GESTE
  - 19 Octobre : Réunion avec le cabinet de Bruno Le Maire : Exposé de la situation. Demander une étude d'impact économique post RGDP / post FAQ

A noter :

Évaluation de l'opportunité de la voie contentieuse : demande de retrait des FAQ sur GA à la CNIL

À date, la seule alternative économiquement viable semble être AT internet, il s'agit du choix fait par les éditeurs ayant désactivé complètement GA, notamment car il permet la transmission certifiée à l'ACPM

La demande de conseil à la CNIL contient une question liée à l'exemption et les transferts hors UE…

Demande de conseil à la CNIL

- Suite aux travaux du GT DPO et de l'Interprofession, nous avons isolé 25 pages de questions pertinentes (+ de 30 points).

- RDV d'une heure pour en parler avec les différents services :
  - Affaires économiques
  - Coordination UE
  - Innovation technologique
- Ce qui démontre que notre demande a été prise en compte

- La durée du RDV ne nous a pas permis d'aborder tous les points, il n'y aura pas de point de suivi. Cf conclusions.

Que peut-on en retenir…

Question 1 : Est-ce un transfert si un prestaire de service dans l'UE soumis à une loi étrangère qui répond à une demande de l'étranger ?

La CNIL explicite la position :

« La soumission à une loi extraterritoriale d'un prestataire de service dans l'UE ne fonde pas l'existence d'un transfert.

Si la réponse à une demande conduit cet acteur à déplacer les données hors UE, et donc un traitement hors UE, alors il y a transfert de données hors UE. »

***Analyse :** Le fait que la demande soit faite au RT ou au ST ne change rien sur l'existence d'un tel transfert, mais celui qui agira sera qualifié d'exportateur.*

digital dpo

Question 2 : quid de la responsabilité du RT qui a recourt à un ST dans l'UE (ex. cloud) qui lui-même utilise un ST ultérieur hors UE.
Dans cette hypothèse, si le transfert est considéré illicite par un régulateur, est-ce que le RT est responsable ?

La CNIL précise que la question discutée en ce moment au niveau du CEPD, pas de décision formelle de la CNIL.

« Ce n'est pas parce que le ST est exportateur responsable de l'encadrement du transfert que le RT n'a pas de responsabilité, car il est en charge de l'encadrement de la sous-traitance selon l'article 28.1, notamment en ce qui concerne les transferts.

Ainsi, dans les CCTs : même si le ST est exportateur, il incombe au RT de définir les mesures encadrant les transferts y compris les mesures additionnelles. »

Limites évoquées mais non tranchées généralement, analyse au cas par cas :

- *Le RT donne ses instructions, mais encore faut-il qu'il ait connaissance des transferts ?*
- *Si 10 000 RT ont recours en UE au même ST dans l'UE qui réalise un transfert vers un STU, dans quelle mesure chacun des RT est-il responsable ? A quel niveau ?*
- *A ce jour l'action de la CNIL est dirigée sur les RT et non sur les ST ou STU, pourquoi ?*

La CNIL indique à nouveau que la responsabilité du RT ne peut être exclue (Art 28.1 RGPD), qu'il doit mener une analyse préalable aux transferts et étudier les mesures.

Délégué à la protection des données

digital dpo

Question 2 : quid de la responsabilité du RT qui a recourt à un ST dans l'UE (ex. cloud) qui lui-même utilise un ST ultérieur hors UE.
Dans cette hypothèse, si le transfert est considéré illicite par un régulateur, est-ce que le RT est responsable ?

Observation Digital DPO sur cette position : *Le RT ne peut être dégagé de sa responsabilité, mais des limites sont à prendre en considération :*

- *Art 28.3 RGPD « Le ST informe immédiatement le RT si, selon lui, une instruction constitue une violation »*
- *Art 28.4 RGPD « Lorsqu'un sous-traitant recrute un autre sous-traitant (…), les mêmes obligations (…) sont imposées par contrat (…) Le ST initial demeure pleinement responsable du respect (…) de ses obligations »*
- *Art 28.10 : « Si (…), un ST détermine les finalités et les moyens d'un traitement, il est considéré comme un RT pour ce qui concerne ce traitement »*

Analyse : *Le RT ne peut être dégagé de sa responsabilité. Quand bien même il est difficile d'arriver à mesurer l'effectivité des mesures de sécurité garantissant un niveau de protection substantiellement équivalent le RT doit effectuer ses « Transfer Impact Assessments » s'il veut être en mesure de se défendre le cas échéant.*

digital dpo

Question 3 : l'évaluation des garanties du prestataire

Lors de l'échange, les mesures complémentaires concrètes, opérationnelles, mobilisables n'ont pas été abordées.

Selon la CNIL, l'évaluation des lois est une 1ère étape, en l'espèce, le droit américain, et notamment FISA, l'a été par la CJUE.

La CNIL dit ne pas être convaincue par un raisonnement basé sur les déclarations historiques ou statistiques des prestataires de services sur l'existence ou non de demandes des autorités, compte tenu qu'ils ont l'obligation de ne pas divulguer le détail de ces demandes.

***Analyse :** Cette position tendrait à conclure, qu'aucun transfert de données vers les US n'est actuellement possible, si des données directement ou indirectement identifiantes sont consultables par les autorités de surveillance US.*
Or la CNIL se refuse à exprimer formellement cette conclusion et maintient en cela le doute… et donc l'incertitude juridique

Question technique subsidiaire : Retour sur la mesure d'audience avec Google Analytics et la proxyfication

La CNIL précise que son but était de dire dans quelle mesure il est encore possible d'utiliser Google Analytics – NDLR : sans transferts hors UE.

Elle reconnait qu'ainsi paramétré il est difficile de répondre au besoin métier.

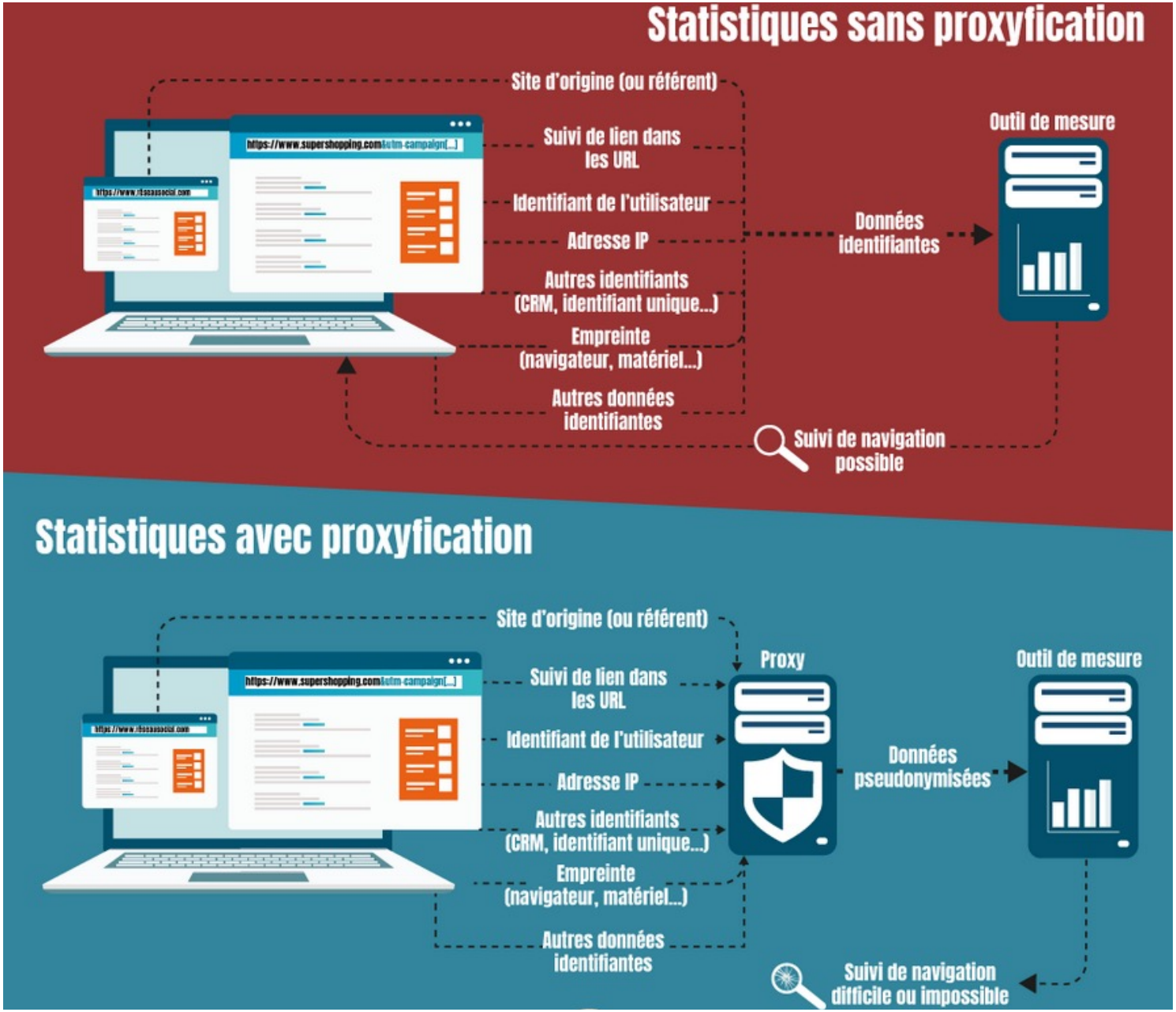
Elle conseille de trouver d'autres solutions qui permettent de répondre aux différents besoins, notamment si l'on souhaite utiliser le referer.

Sollicitée sur l'importance de la mesure d'audience certifiée pour les éditeurs et sur l'existence d'alternatives, en substance la CNIL nous répond :

- *en avoir conscience, travailler sur le sujet*
- *ne pas pouvoir réévaluer son programme d'exemption lié à la mesure d'audience (ePrivacy) avec cette donnée*
- *Rappel que les solutions autohébergées apportent des garanties fortes, malgré des fonctionnalités manquantes*

Analyse : *A doctrine constante, il ne semble pas y avoir grand-chose à attendre de la CNIL sur le sujet.*

Proxyfication / Conditions CNIL



digital dpo

Proxyfication / Conditions CNIL

Selon la CNIL, les mesures nécessaires à mettre en place pour que la *proxyfication* soit valable :

- **Non transfert de l'adresse IP**
- **Non transfert de l'identifiant utilisateur** (utilisation d'un hash avec variable temporelle aléatoire)
- **Non transfert du référer**
- **Suppression de tout paramètre dans les URL** (UTM, index internes)
- **Altération des informations pouvant générer d'une empreinte** (ou *fingerprint*)
- **Non transfert de tout identifiant *cross-site* ou déterministe** (CRM, UID)
- **Suppression de toute autre donnée pouvant mener à une réidentification**

Analyse : Ainsi définis, les flux de données ne contiennent plus de données personnelles ou elles ont été altérées de manière telles qu'une réidentification est impossible. **Re-targetting et activation externe sont donc très limités.**