La Newsletter dédiée à la mise en conformité au RGPD

par @DerriennicParis

DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 25

Madame, Monsieur,

La période estivale qui s'achève a été marquée par un arrêt de la Cour de justice de l'Union européenne dont on peine encore à mesurer les implications sur les transferts de données vers les Etats-Unis. Nous vous proposons, en ce mois de septembre 2020, de découvrir les tenants et aboutissants de cet arrêt, nos recommandations sur le sujet, ainsi que d'autres actualités que nous avons sélectionnées pour vous en rapport avec la protection des données à caractère personnel :

- Le Privacy Shield invalidé par la CJUE ;
- Invalidation du Privacy Shield : quelques recommandations ;
- Invalidation du Privacy shield : La FAQ du CEPD
- Mise en garde de la CNIL contre la verbalisation par lecture automatisée des plaques d'immatriculation
- Le Conseil d'Etat invalide l'interdiction des « cookie walls » posée par la CNIL ;
- La CNIL publie six bonnes pratiques à destination des responsables de traitement et sous-traitants.

Nous vous en souhaitons une bonne lecture.

Le Privacy Shield invalidé par la CJUE

La CJUE a rendu un arrêt, le 16 juillet 2020, dans lequel elle a invalidé la décision relative à l'adéquation de la protection assurée par le bouclier de protection des données EU-Etats-Unis.

La Haute Cour irlandaise, saisie par un particulier qui souhaitait interdire à Facebook Ireland de transférer des données à caractère personnel vers les Etats-Unis, a décidé de surseoir à statuer et de poser à la Cour de justice de l'Union européenne (CJUE) plusieurs questions préjudicielles, amenant la CJUE à se prononcer, dans un arrêt du 16 juillet 2020, sur la validité des décisions 2010/87 (relative aux clauses contractuelles types) et 2016/1250 (relative à l'adéquation de la protection assurée par le bouclier de protection des données EU-Etats-Unis dit « *Privacy shield* »).

S'agissant de la décision 2010/87 portant sur les clauses contractuelles types, sa validité n'a pas été remise en cause par la CJUE. En effet, bien que ces clauses ne lient pas les autorités du pays tiers vers lequel le transfert de données pourrait être opéré, la décision 2010/87 comporte des mécanismes effectifs permettant, en pratique, d'assurer que le niveau de protection requis par le droit de l'Union soit respecté et que les transferts soient suspendus ou interdits en cas de violation des clauses ou d'impossibilité de les honorer.

La CJUE a, par ailleurs, affirmé le principe selon lequel, en l'absence de décision d'adéquation, les autorités de contrôles sont obligées de suspendre ou d'interdire un transfert de données à caractère personnel vers un pays tiers lorsqu'elles estiment, au regard des circonstances propres à ce transfert, que les clauses types de protection des données ne sont pas ou ne peuvent pas être respectées dans ce pays et que la protection des données transférées, requise par le droit de l'Union, ne peut pas être assurée par d'autres moyens, à défaut pour l'exportateur établi dans l'Union d'avoir lui-même suspendu ou mis fin à un tel transfert.

S'agissant de la décision 2016/1250 relative au Privacy Shield, la CJUE a indiqué que les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, des données transférées depuis l'UE vers les Etats-Unis, ne sont pas encadrées d'une manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union, par le principe de proportionnalité, en ce que les programmes de surveillance fondés sur cette réglementation ne sont pas limités au strict nécessaire.

De plus, s'agissant de l'exigence de protection juridictionnelle, la CJUE a jugé que le mécanisme de médiation lié au Privacy Shield ne fournit pas aux personnes concernées une voie de recours devant un organe offrant des garanties substantiellement équivalentes à celles requises en droit de l'Union, de nature à assurer tant l'indépendance du médiateur prévu par ce mécanisme que l'existence de normes habilitant ledit médiateur à adopter des décisions contraignantes à l'égard des services de renseignement américains.

Pour ces deux raisons, la CJUE a déclaré la décision 2016/1250 invalide.

La CNIL a annoncé, au lendemain de cette décision, procéder à une analyse précise de cette dernière, en lien avec les autres autorités du CEPD, afin « *d'en tirer les conséquences pour les transferts de données de l'Union européenne vers les Etats-Unis* ».

Lien vers l'arrêt de la CJUE :

http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=9978398

Lien vers la publication de la CNIL :
https://www.cnil.fr/fr/invalidation-du-privacy-shield-la-cnil-et-ses-homologues-analysent-actuellement-ses-consequences

Invalidation du Privacy Shield : quelques recommandations

Suite à l'invalidation du mécanisme de Privacy Shield, voici quelques recommandations concernant les garanties à apporter aux transferts de données à caractère personnel à destination des Etats-Unis.

La décision relative à l'adéquation de la protection assurée par le Privacy Shield a été invalidée par la Cour de justice de l'Union européenne (CJUE), dans une décision du 16 juillet 2020 (affaire C-311/18) qui a fait l'objet d'un article sur notre site internet.

La CJUE a en effet considéré que les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis ne sont pas encadrées d'une manière à répondre à des exigences substantiellement équivalentes à celles requises en droit de l'Union.

Les transferts vers les Etats-Unis ne peuvent donc plus être considérés comme conformes au RGPD sur la base du Privacy Shield.

La CJUE, si elle a confirmé la validité de la décision relative aux clauses contractuelles types, a précisé à leur égard qu'une autorité de contrôle telle que la CNIL doit suspendre un transfert fondé sur ces clauses, « *lorsque cette autorité de contrôle considère, à la lumière de l'ensemble des circonstances propres à ce transfert, que ces clauses ne sont pas ou ne peuvent pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union […] ne peut pas être assurée par d'autres moyens, à défaut pour le responsable du traitement ou son sous-traitant établis dans l'Union d'avoir lui-même suspendu le transfert ou d'avoir mis fin à celui-ci* ».

Ainsi, les clauses contractuelles types demeurent une alternative incertaine au Privacy Shield, dans la mesure où elles ne présentent aucun caractère contraignant vis-à-vis des autorités américaines.

La CNIL a annoncé, au lendemain de cette décision, procéder à une analyse précise de la décision de la CJUE, en lien avec les autres autorités du CEPD, afin « *d'en tirer les conséquences pour les transferts de données de l'Union européenne vers les Etats-Unis* ». Le CEPD a, pour sa part, annoncé réfléchir à des mesures supplémentaires à mettre en œuvre par l'expéditeur des données, qui viendraient compléter les clauses contractuelles types.

Nous restons donc dans l'attente de leur position.

Dans l'intervalle, le cabinet souhaite souligner le fait qu'un transfert de données à caractère personnel vers les Etats-Unis présente un risque de non-conformité au RGPD substantiel, quel que soit le mécanisme de transfert auquel l'exportateur a recours, et recommande de ne pas procéder à un tel transfert lorsque cela est possible.

Si, néanmoins, un transfert de données vers les Etats-Unis est inévitable, le cabinet recommande de :

- conclure des clauses contractuelles types avec l'importateur de données, pour les transferts précédemment couverts par le Privacy Shield, mais également pour les futurs transferts « inévitables » ;
- dans la mesure où cela est possible, chiffrer ou pseudonymiser les données avant leur transfert, sans laisser à l'importateur la possibilité de les déchiffrer ou d'identifier la personne concernée. Cette option n'est, néanmoins, pas envisageable dans tous les cas de figure et pourra être refusée par l'importateur.

Ces actions nécessiteront également de mettre à jour les mentions d'information, le registre des traitements et les éventuelles analyses d'impact.

Un audit préalable des contrats pourra permettre d'identifier les transferts de données à caractère personnel à destination des Etats-Unis.

Lien vers la décision de la CJUE :
http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=9978398

Invalidation du Privacy shield : La FAQ du CEPD

Suite à l'arrêt de la Cour de justice de l'Union européenne (CJUE) dans le cadre de l'affaire « Schrems II » ayant invalidé le Privacy Shield, le Comité européen de protection des données (CEPD) a délivré ses premiers éléments de réponse aux questions les plus fréquemment posées.

La CNIL, dans une publication du 31 juillet 2020, a traduit la FAQ produite par le CEPD au sujet de l'invalidation du Privacy Shield par la CJUE.

Il y est indiqué les éléments suivants :

1. Le CEPD a confirmé qu'il n'y aurait pas délai de grâce pendant lequel les entités pourraient continuer à transférer des données aux Etats-Unis sans évaluer la base légale du transfert.

2. Le recours aux clauses contractuelles types (CCT), de même qu'aux règles d'entreprise contraignantes (BCR), nécessite, selon le CEPD, de procéder à une évaluation prenant en compte les circonstances du transfert et les mesures supplémentaires que l'exportateur de données pourrait mettre en place. L'ensemble formé par ces mesures supplémentaires et les CCT (ou les BCR), après une analyse au cas par cas des circonstances entourant le transfert, devra garantir que la législation américaine ne compromet pas le niveau de protection adéquat que les clauses et ces mesures garantissent.

Le CEPD analyse actuellement l'arrêt de la Cour afin de déterminer le type de mesures complémentaires qui pourraient être fournies en plus des CCT ou des BCR, qu'il s'agisse de mesures juridiques, techniques ou organisationnelles, pour transférer des données vers des pays tiers dans lesquels les CCT ou les BCR ne fourniront pas à elles-seules le niveau de garanties suffisant.

S'il résulte de l'évaluation diligentée par l'exportateur, que le respect des garanties appropriées ne serait pas assuré, l'exportateur sera tenu de suspendre ou de mettre fin au transfert de données. S'il a l'intention de continuer à transférer des données en dépit de cette conclusion, l'exportateur devra « *notifier l'autorité de contrôle compétente* ».

3. S'agissant des dérogations prévues à l'article 49 du RGPD (consentement de la personne concernée, transfert nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, etc.), le CEPD a indiqué qu'un transfert sur leur base est possible, dès lors que les conditions énoncées dans cet article s'appliquent. Le CEPD a également rappelé le principe selon lequel ces dérogations ne doivent pas devenir « la règle » dans la pratique, mais doivent être limitées à des situation spécifiques, chaque exportateur devant s'assurer que le transfert réponde au critère de stricte nécessité.

4. Le CEPD a abordé, dans cette FAQ, le cas des responsables du traitement ayant conclu un contrat avec un sous-traitant prévoyant la possibilité d'un transfert de données vers les Etats-Unis ou vers un autre pays tiers.

Selon le CEPD, si les données peuvent être, en application de ce contrat, ainsi transférées aux États-Unis et qu'aucune mesure supplémentaire ne peut être prévue pour garantir que la législation américaine n'affecte pas le niveau de protection essentiellement équivalent à celui offert dans l'EEE par les outils de transfert, ni qu'aucune dérogation au titre de l'article 49 du RGPD ne s'applique, « *la seule solution est de négocier un avenant ou une clause supplémentaire au contrat pour interdire les transferts vers les États-Unis* ». Les données devront alors être stockées et administrées ailleurs qu'aux États-Unis.

Si les données peuvent être transférées vers un autre pays tiers, le responsable du traitement

devra, selon le CEPD, vérifier la législation de ce pays tiers pour s'assurer qu'elle est conforme aux exigences de la CJUE et au niveau de protection des données personnelles attendu. Si aucune base légale de transfert vers un pays tiers ne peut être trouvée, les données personnelles ne devront pas être transférées en dehors du territoire de l'EEE et toutes les activités de traitement devront avoir lieu dans l'EEE.

Lien vers la publication de la CNIL :
https://www.cnil.fr/sites/default/files/atoms/files/faq_privacy-shield-invalidation_edpb_en.pdf

Lien vers le document original du CEPD :
https://www.cnil.fr/sites/default/files/atoms/files/faq_privacy-shield-invalidation_edpb_en.pdf

Mise en garde de la CNIL contre la verbalisation par lecture automatisée des plaques d'immatriculation

Dans une publication du 25 août 2020, la CNIL a indiqué avoir mis en demeure des communes de se conformer au cadre légal en matière de lecture automatisée des plaques d'immatriculation, et plus particulièrement de cesser la collecte de fichiers photographiques.

La CNIL a constaté, dans le cadre de ses contrôles, que des collectivités locales avaient automatisé le processus de verbalisation des infractions, en faisant équiper les véhicules de police municipale de caméras dotées d'un dispositif de lecture automatisée des plaques d'immatriculation (LAPI), afin de permettre la collecte automatique de données des véhicules en infraction.

La CNIL a indiqué, dans une publication du 25 août 2020, que si l'arrêté du 14 avril 2019 prévoit la possibilité de recourir à de tels dispositifs dans le cadre du contrôle du forfait post-stationnement, néanmoins, il ne permet pas la collecte de fichiers photographiques. Ainsi, la collecte et le traitement de photographies des véhicules, pour l'exercice du pouvoir de police par les communes (en lien avec la tranquillité publique ou la salubrité publique), ne sont pas autorisés en l'état actuel de la règlementation.

La CNIL a indiqué, dans sa publication, que sa présidente et sa vice-présidente avaient adopté plusieurs mises en demeure à l'encontre de communes ne respectant pas ce cadre légal.

Lien vers la publication de la CNIL :
https://www.cnil.fr/fr/verbalisation-par-lecture-automatisee-des-plaques-dimmatriculation-lapi-la-cnil-met-en-garde

Le Conseil d'Etat invalide l'interdiction des « cookie walls » posée par la CNIL

La date d'adoption du règlement ePrivacy se faisant attendre, la CNIL avait, par une délibération n° 2019-093 du 4 juillet 2019, établi des lignes directrices sur les « cookies et autres traceurs ».

Diverses associations professionnelles avaient saisi le Conseil d'État (ci-après le « CE ») d'une requête tendant, à titre principal, à l'annulation pour excès de pouvoir de cette délibération.

Les requérants critiquaient la délibération sur les points suivants :

- La régularité de la procédure d'adoption de la délibération,

- La compétence de la CNIL pour prendre une telle délibération,

- Le régime applicable aux « cookies » et autres traceurs de connexion,

- L'interdiction des « cookie walls »,

- L'indépendance, la spécificité et le caractère éclairé du consentement,

- Les autres obligations formulées par la délibération attaquée (conditions de refus du consentement, conditions pour bénéficier de l'exemption et l'information sur les cookies et autres traceurs non-soumis au consentement).

Dans sa décision du 19 juin 2020, le CE a rejeté la majorité des griefs des requérants mais a considéré que l'interdiction des « cookie walls » entachait les lignes directrices d'illicéité.

Dans sa décision, le CE a confirmé la compétence de la CNIL pour adopter des « lignes directrices » applicables en matière de « cookies » et autres traceurs. La haute juridiction a également précisé que la CNIL pouvait faire application aux « cookies » et autres traceurs, du régime du consentement requis par le RGPD.

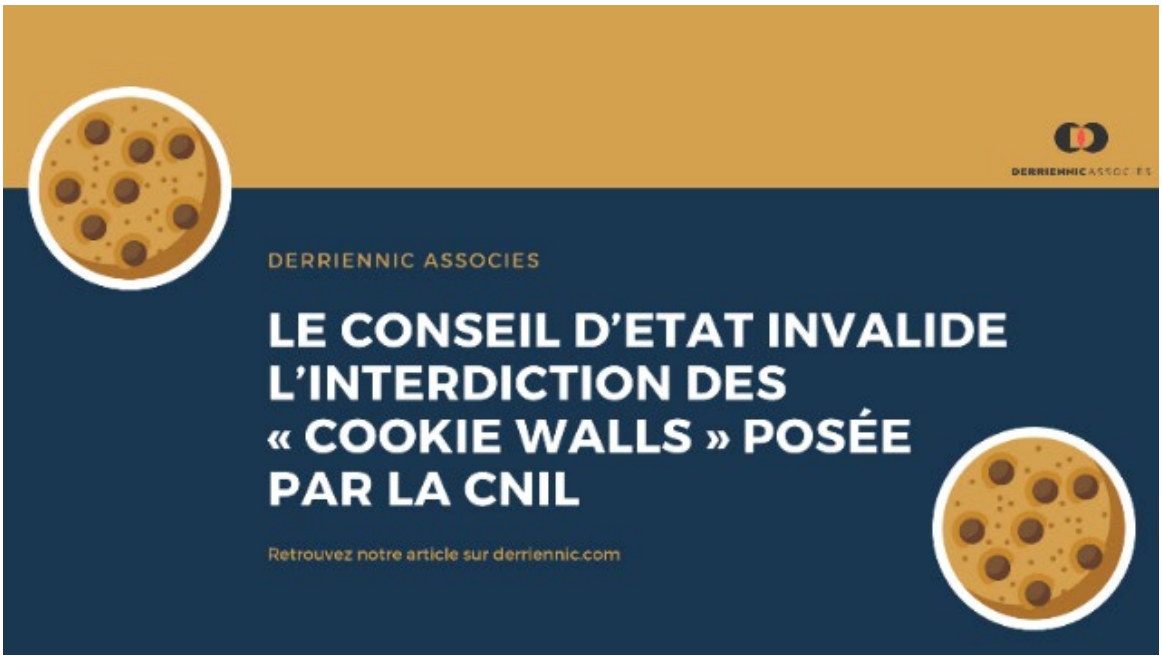
En revanche, un point des lignes directrices est sanctionné. Il concerne l'interdiction des « cookie walls ». La CNIL avait en effet considéré comme non-conforme le fait que l'accès à un site internet soit subordonné à l'acceptation des cookies (« cookie walls »).

En déduisant une telle interdiction générale et absolue des « cookie walls » de la seule exigence d'un consentement libre posé par le RGPD, le CE a considéré que « la CNIL a excédé ce qu'elle peut légalement faire, dans le cadre d'un instrument de droit souple » et déclare la délibération attaquée entachée d'illégalité.

Le CE sanctionne donc le fait que la CNIL ait outrepassé ce qui lui était possible de faire dans le cadre d'un instrument de « droit souple ».

Dans son communiqué, le CE précise en effet que « Les actes de droit souple désignent les instruments, telles que les lignes directrices des autorités de régulation, qui ne créent pas de droit ou d'obligation juridique pour quiconque mais influencent fortement, dans les faits, les pratiques des opérateurs économiques. Sans se prononcer sur le fond de la question, le Conseil d'État considère que la CNIL ne pouvait, sous couvert d'un acte de droit souple, énoncer une telle interdiction générale et absolue. »

Lien vers la décision du CE :
https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-lignes-directrices-de-la-cnil-relatives-aux-cookies-et-autres-traceurs-de-connexion



La CNIL publie six bonnes pratiques à destination des responsables de traitement et sous-traitants

Le 9 juillet dernier, dans le prolongement de vérifications réalisées auprès de 15 fournisseurs de services et solutions informatiques en ligne (sans qu'aucune précision ne soit faite sur ces vérifications), la CNIL a publié des bonnes pratiques à destination des responsables de traitement et des sous-traitants.

Pour mémoire, le règlement 2016/679 (ci-après « RGPD ») impose des obligations aux responsables de traitement et sous-traitants.

Afin d'accompagner les entreprises agissant comme sous-traitant, au sens du RGPD, la CNIL avait publié un guide à leur attention en septembre 2017 (accessible ici). Dans le prolongement de ce guide, la CNIL propose six bonnes pratiques adressées aux responsables de traitement et aux sous-traitants.

A ce titre, la CNIL recommande de :

• Déterminer le statut des acteurs impliqués, le cas échéant, en qualifiant la relation de sous-traitance au sens du RGPD ;

• Etablir un contrat clair, incluant les mentions obligatoires de l'article 28 du RGPD. A cet égard, la CNIL recommande de porter une attention particulière à la définition et l'encadrement du traitement de données à caractère personnel ainsi qu'aux conditions de recours à la sous-traitance ultérieure ;

• Documenter l'activité de sous-traitance, en (i) veillant à ce que les instructions données par le responsable de traitement soient formalisées par écrit, (ii) tenant un registre des activités de traitement réalisées pour le compte du responsable de traitement et, (iii) veillant à ce que le sous-traitant mette à disposition les informations nécessaires à la démonstration du respect de ses obligations et à la réalisation d'audit ;

• Proposer des outils respectueux des données à caractère personnel, comme une interface de recueil du consentement, un lien de désinscription automatique, une interface et un modèle d'information des personnes ou, un système de purge automatique des données dont la durée de conservation serait arrivée à son terme ;

• Aider le responsable de traitement à répondre aux demandes d'exercice des droits des personnes concernées, notamment grâce à la mise en place d'une interface d'exercice des droits des personnes permettant le suivi et la répartition automatique des demandes d'exercice des droits en fonction de leur objet ; et

• Garantir la sécurité des données collectées, par exemple en exigeant la communication par le prestataire de sa politique de sécurité des systèmes d'information (PSSI), mettant en œuvre des audits de sécurité, ou des certifications de l'organisme et/ou de son personnel.

Enfin, la CNIL indique que le Comité européen de la protection des données est en cours de rédaction de travaux sur les notions de responsables de traitement et sous-traitant. Une fois publiés, ces travaux compléteront ainsi les présentes recommandations.

Lien vers la publication :
https://www.cnil.fr/fr/responsable-de-traitement-et-sous-traitant-6-bonnes-pratiques-pour-respecter-les-donnees