

Les dernières actualités RGPD sélectionnées par le cabinet Vigo, à destination des DPO, responsables juridiques, auditeurs ainsi que leurs relais de conformité internes.



ACTUALITÉS RGPD : CE QU'IL FAUT RETENIR POUR LA RENTRÉE



Cet été, l'activité de la CNIL s'est poursuivie et plusieurs délibérations de sanctions ont ainsi été rendues pour non-respect des dispositions du Règlement Général sur la Protection des Données (ci-après « RGPD »).

L'autorité française de contrôle a également profité de la période estivale pour adresser une deuxième série de mises en demeure sur l'une de ses thématiques prioritaires pour 2021, à savoir l'utilisation des cookies¹.

Voici ce qu'il faut retenir pour être à jour des actualités relatives à la réglementation française et européenne en matière de protection des données à caractère personnel et de cookies.

Dans l'Union européenne, deux actualités ont également attiré notre attention : l'amende record infligée à Amazon par l'autorité de contrôle luxembourgeoise et l'adoption définitive des lignes directrices du Comité européen de protection des données (CEPD) sur les notions de responsable de traitement et de sous-traitant.

I. Actualités CNIL

21 juin 2021 - RGPD et cookies : sanction de 500 000 euros à l'encontre de la société BRICO PRIVE²

Plusieurs manquements au RGPD constatés : non-respect des durées de conservation des données (article 5.1.e du RGPD) ; de l'obligation d'information des personnes (article 13 du RGPD) ; du droit à l'effacement (article 17 du RGPD) ; de l'obligation d'assurer la sécurité des données à caractère personnel (article 32 du RGPD).

- **S'agissant de l'information des personnes** : l'article 13 prévoit une liste de mentions obligatoires à mettre à la disposition des personnes concernées. La CNIL rappelle dans cette délibération qu'une rubrique « désabonnement et désinscription » n'est pas suffisante pour permettre aux personnes concernées de s'adresser au délégué à la protection des données (DPO) et d'exercer leurs droits.



À retenir : les coordonnées du DPO doivent être indiquées précisément, dans les conditions générales de vente, les mentions légales et/ou la politique de confidentialité. Il convient en outre de créer une adresse de contact spécifique (et générique) pour le DPO.

¹ Voir [le communiqué de presse de la CNIL](#) en date du 19 juillet 2021

² Délibération SAN-2021-008 du 14 juin 2021.

- **S'agissant du droit à l'effacement** : la CNIL rappelle que l'effacement des données implique pour la société de procéder à la suppression des données à caractère personnel et non pas seulement à la désactivation du compte de la personne concernée.
- **S'agissant de l'obligation d'assurer la sécurité des données à caractère personnel** : la CNIL rappelle que la force d'un mot de passe assurant la sécurité repose sur la longueur et la complexité de celui-ci.



À retenir : un manquement à cette obligation peut être sanctionné, même en l'absence de violation de données. Retrouvez [les conseils de la CNIL](#) pour un mot de passe solide.

- **S'agissant de la prospection commerciale et des cookies** : la CNIL a également constaté des manquements aux règles de prospection commerciale et à celles relatives aux cookies.



À retenir : pas de message commercial, publicité ou prospection commerciale par courrier électronique sans accord préalable du destinataire ! Assurez-vous donc que le consentement préalable des utilisateurs de votre site est bien recueilli, notamment par le biais d'une case à cocher. Attention, pour que le consentement soit valide, la case ne doit pas être « pré-cochée ».

SOURCE

26 juillet 2021 - Fichier de lobbying : Sanction de 400 000 euros à l'encontre de la société MONSANTO³

Dans le cadre de ses activités de lobbying, la société MONSANTO a fait appel à deux sociétés spécialisées en affaires publiques, lesquelles ont recensé près de 200 personnalités politiques susceptibles d'intervenir dans le processus décisionnel, sans que ces dernières n'en aient été informées.

Or, bien que des exceptions existent à l'obligation d'information en cas de collecte indirecte des données (article 14, 5. du RGPD), le Conseil d'État et la CNIL reconnaissent rarement leur application. Ainsi, l'information par le responsable de traitement n'est pas considérée comme un « effort disproportionné » dès lors que ce dernier dispose d'un moyen de contact des personnes concernées, même si cela représente 25 millions⁴ de personnes.



À retenir : même en cas de collecte indirecte des données, les personnes concernées doivent être informées des modalités de traitement.

Par ailleurs, la CNIL reproche à la société MONSANTO le défaut d'encadrement des traitements effectués par ses sous-traitants par un acte juridique formalisé (article 28 du RGPD). Le traitement des données effectué par un sous-traitant doit être régi par un contrat ou un autre acte juridique. Ce document contractuel doit obligatoirement contenir un certain nombre d'informations relatives au traitement, notamment l'objet, la durée, la finalité, etc.

³ Délibération SAN-2021-012 du 26 juillet 2021.

⁴ [Conseil d'État, 10ème et 9ème sous-sections réunies, 12/03/2014, 353193](#)



À retenir : en qualité de responsable de traitement, vous devez vous assurer que les traitements effectués par des sous-traitants répondent aux exigences du RGPD. Il convient donc, d'abord, d'identifier ces traitements puis de conclure un contrat incluant lesdites mentions obligatoires. Cela vous permettra d'organiser les rapports et obligations respectives.

SOURCE

27 juillet 2021 - Cookies tiers : sanction de 50 000 euros à l'encontre de la SOCIÉTÉ DU FIGARO⁵

À la suite d'une saisine de la CNIL au sujet du dépôt de cookies publicitaires sur le terminal d'un utilisateur, avant toute action de sa part sur le site, et sans recueil de son consentement, la SOCIÉTÉ DU FIGARO a été condamnée à 50 000 euros d'amende. La responsabilité de la société DU FIGARO a été reconnue alors même que le dépôt de cookies était réalisé par des tiers à partir des sites édités par la société DU FIGARO dans la mesure où :

- Le code des sites internet permettait à des tiers de déposer des cookies via les sites DU FIGARO ;
- Les mesures mises en place par la société DU FIGARO : outil de gestion du consentement et veille, ne sont pas suffisantes pour répondre à l'obligation de moyen à laquelle cette dernière est soumise.

Points d'attention :

- Les éditeurs de site web ont l'obligation de s'assurer que le dépôt de cookies par les sociétés tierces respecte la réglementation en vigueur (RGPD ; article 82 de la Loi Informatique et Libertés ; lignes directrices et recommandations de la CNIL).
- La réglementation en matière de cookies implique de respecter les dispositions du RGPD, mais également les nouvelles lignes directrices et la recommandation de la CNIL, en date du 1^{er} octobre 2020.
- La mise en place d'une plateforme de gestion du consentement et une politique de cookies sont des éléments indispensables dans votre mise en conformité. En revanche, ils ne sont pas suffisants dès lors que des tiers ont la possibilité de déposer des cookies via votre site internet.



À retenir : dès lors que des cookies tiers peuvent être déposés sur le terminal des utilisateurs à partir de votre site, assurez-vous que les traceurs respectent la réglementation applicable en France par tous moyens, notamment en effectuant toute démarche utile auprès d'eux pour mettre fin à d'éventuels manquements :

- *Audit (avec CookieViz par exemple) ;*
- *Mise en demeure / Résiliation du contrat avec le tiers.*

Pour en savoir plus, retrouvez [ici](#) notre webinaire sur le sujet.

SOURCE

II. Et en Europe ?

⁵ Délibération SAN-2021-013 du 27 juillet 2021.

16 juillet 2021 - Sanction record de 746 millions d'euros infligée à Amazon par l'autorité de contrôle luxembourgeoise

En 2018, une plainte collective rassemblant plus de 10 000 personnes et initiée par la Quadrature du Net avait été déposée en 2018 afin de dénoncer un traitement de données personnelles sans base légale afin de réaliser des analyses comportementales et un ciblage publicitaire par la société Amazon. L'autorité de contrôle luxembourgeoise a condamné cette dernière, en juillet dernier, à une amende record de 746 millions d'euros.

En raison des règles procédurales luxembourgeoises, la décision n'est pas encore disponible.

SOURCE

7 juillet 2021 - Adoption des lignes directrices du CEPD sur les notions de responsables de traitement et de sous-traitant⁶

Le CEPD (Comité européen à la protection des données) a adopté la version finale de ses lignes directrices sur les notions de responsable de traitement et sous-traitant dans le cadre du RGPD. Ces lignes directrices permettent d'apporter des indications pratiques afin d'identifier concrètement les différents acteurs de traitement des données à caractère personnel ainsi que leurs obligations.

Ainsi, à titre d'exemple, le responsable de traitement est celui qui détermine les finalités et les moyens du traitement. Le CEPD précise qu'il convient d'effectuer une analyse au cas par cas, notamment lorsque certains moyens du traitement relèvent du sous-traitant. À noter que pour le CEPD, la finalité du traitement est toujours du ressort du responsable de traitement.

À cet égard, il convient de distinguer entre moyens essentiels et non essentiels au traitement. Les moyens essentiels touchant à la finalité du traitement sont réservés au responsable du traitement tandis que les moyens non essentiels peuvent relever de l'appréciation du sous-traitant.

Attention aux notions de « prestataire » et de « sous-traitant » : le prestataire n'est pas nécessairement sous-traitant au sens du RGPD, mais peut être responsable ou responsable conjoint.



À retenir : les contrats, obligatoires entre les différents acteurs d'un traitement, doivent être rédigés au cas par cas, en tenant compte des spécificités de chaque traitement et en détaillant précisément les responsabilités de chaque acteur.

SOURCE

28 juin 2021 – Décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données personnelles assuré par le Royaume Uni⁷

Le 28 juin 2021, la Commission européenne a adopté deux décisions d'adéquation relatives aux transferts de données personnelles vers le Royaume-Uni, l'une au titre du RGPD et l'autre au titre de la directive afférente à la protection des données dans le domaine répressif.

⁶ [Guidelines 07/2020 on the concepts of controller and processor in the GDPR](#) (uniquement en anglais).

⁷ [Décision d'exécution de la Commission du 28 juin 2021 constatant, conformément au règlement 2016/679 du Parlement européen et du Conseil, le niveau adéquat des données à caractère personnel assuré par le Royaume-Uni](#)



À retenir : *les transferts de données personnelles depuis l'Union européenne vers le Royaume-Uni peuvent être mis en œuvre sans garanties ou conditions supplémentaires.*

SOURCE

Équipe Protection des données et cybercriminalité – Emmanuel DAOUD, Imane BELLO, Yuna LESTEVEN et Emma JALLOUL

Le Cabinet VIGO propose un accompagnement dans les domaines de la protection des données personnelles, la cybercriminalité, la cybersécurité. Conscients des nouveaux enjeux liés aux évolutions technologiques, mais aussi de la multitude de textes juridiques pouvant complexifier vos méthodes de travail et l'organisation de votre entreprise, nos avocats spécialisés vous apporteront conseil et assistance, n'hésitez pas à nous contacter !

Vous recevez ce message car notre cabinet vous considère comme intéressé(e) par l'actualité qu'il publie. Vous pouvez vous désabonner à tout moment en cliquant sur le lien prévu à cet effet.