Newsletter Compliance

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

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

Ces derniers mois, l'activité de la CNIL s'est poursuivie et plusieurs délibérations de sanctions ont été rendues pour non-respect des dispositions du Règlement Général sur la Protection des Données (ci-après « RGPD ») ou de la réglementation en matière de cookies.

Ainsi, la CNIL a poursuivi ses contrôles et adressé une trentaine de nouvelles mises en demeure pour non-conformité à la réglementation en matière de cookies. Elle a également sanctionné les sociétés Google Ireland Limited, Google LLC et Facebook Ireland Limited pour manquement à la réglementation en matière de cookies.

La société FREE MOBILE a quant à elle été sanctionnée pour manquements au RGPD relatifs au droit des personnes et à la sécurité des données ; tandis que la société SLIMPAY a notamment été sanctionnée pour défaut d'information aux personnes concernées suite à une violation de données

Dans l'Union européenne, trois actualités ont également attiré notre attention : l'amende record infligée à la société GRINDR par l'autorité de contrôle norvégienne, la décision d'un tribunal civil allemand d'accorder une réparation civile à la suite d'une violation du RGPD et la décision d'adéquation de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par la République de Corée.

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 en cette rentrée 2022.

I. Actualités CNIL

31 décembre 2021 – Cookies : sanction par la CNIL des sociétés GOOGLE IRELANCE LIMITED, GOOGLE LLC[1] et FACEBOOK IRELAND LIMITED[2]

À la suite de différents contrôles, la CNIL a constaté que les sites web facebook.com, google.fr et youtube.com proposaient un bouton permettant d'accepter immédiatement les cookies. En revanche,

[1] Délibération SAN-2021-023 du 31 décembre 2021
[2] Délibération SAN-2021-024 du 31 décembre 2021

ils ne mettaient pas en place de solution équivalente (bouton ou autre) pour permettre à l'internaute de refuser facilement le dépôt de ces cookies.

Le 31 décembre 2021, la pratique relative à la mise en place de plusieurs clics pour refuser tous les cookies, tandis qu'un seul est nécessaire pour les accepter, a été considérée comme portant atteinte à la liberté du consentement par la CNIL, et subséquemment comme constituant une violation de l'article 82 de la loi Informatique et Libertés.

Deux amendes ont été prononcées à l'encontre de GOOGLE, l'une d'un montant de 90 millions d'euros pour GOOGLE LLC et l'autre d'un montant de 60 millions d'euros pour GOOGLE IRELAND LIMITED ; tandis que la société FACEBOOK IRELAND LIMITED s'est vu imposer une amende d'un montant de 60 millions d'euros.

L'autorité a notamment justifié le montant des amendes par les bénéfices tirés des revenus publicitaires indirectement générés à partir des données collectées par les cookies.

À ces amendes s'ajoutent une injonction sous astreinte de mettre à disposition des internautes situés en France, dans un délai de trois mois un moyen permettant de refuser les cookies aussi simplement que celui existant pour les accepter. Passé ce délai les sociétés devront chacune payer une astreinte de 100.000 euros par jour de retard.

Perspectives *: Depuis le 31 mars 2021, date à laquelle le délai accordé par la CNIL aux sites et applications mobiles pour se mettre en conformité avec les règles en matière de cookies est écoulé, la CNIL a adopté une centaine de mesures correctrices (sanctions ou mises en demeure). Il est à prévoir que son action en la matière continuera en 2022. Il faut donc porter une attention particulière à cette réglementation et s'assurer que, pour l'utilisateur, refuser les cookies soit aussi simple que les accepter.*

À défaut, les sociétés déposant des cookies sur les terminaux des internautes situés en France dans le cadre de l'activité d'un établissement sur le territoire français pourraient être sanctionnées par la CNIL.

En effet, les opérations liées à l'utilisation des cookies relèvent de la directive transposée à l'article 82 de la loi Informatique et Libertés. En ce sens, et puisque le recours aux cookies est effectué dans le cadre des activités de la société Google France qui constitue l'établissement sur le territoire français des sociétés Google LLC et Google Ireland Limited, la CNIL doit être considérée comme territorialement compétente. Elle est par ailleurs matériellement compétente pour contrôler et sanctionner les opérations liées aux cookies déposés par les sociétés sur les terminaux internautes situés en France.

SOURCE

SOURCE

28 décembre 2021 – Prospection commerciale : droits des personnes concernées, protection dès la conception et sécurité des données : sanction de 300 000 euros à l'encontre de la société FREE MOBILE[3]

[3] Délibération SAN-2021-021 du 28 décembre 2021.

Entre fin 2018 et fin 2019, la CNIL a été saisie d'une vingtaine de plaintes afférentes aux difficultés rencontrées par des personnes concernées dans l'exercice de leurs droits d'accès ou d'opposition à recevoir des messages de prospection commerciale.

La CNIL considère que certaines plaintes déposées constituent un manquement au droit d'accès prévu par les articles 12 et 15 du RGPD, et ce, peu important que les manquements n'aient pas de caractère structurel (en l'espèce, les manquements concernent un petit nombre de personnes). La CNIL considère également que le défaut de prise en compte d'une demande d'opposition, le défaut de réponse ou le retard dans le traitement d'une telle demande contreviennent à l'obligation posée à l'article 21 du RGPD.

De surcroît, l'autorité relève que si une donnée n'est pas essentielle dans le cadre du traitement pour laquelle elle est utilisée (en l'espèce, un identifiant aurait permis de remplir l'objectif poursuivi par l'utilisation de la donnée en question) , un manquement au principe de protection des données dès la conception peut être caractérisé. Elle condamne ainsi la société FREE MOBILE sur ce fondement au regard du caractère obsolète d'une donnée utilisée dans le cadre de l'émission des facturations en cours.

Enfin, la CNIL indique que son guide relatif à la sécurité des données à caractère personnel et la note technique de l'ANSSI relative aux mots de passe, s'ils n'ont pas de caractère impératif, doivent être compris comme exposant les précautions élémentaires de sécurité correspondant à l'état de l'art. L'autorité considère en l'état que les mesures de sécurité prises étaient insuffisantes et caractérisent seules (sans l'existence d'une violation de données), par leur caractère lacunaire, un manquement à l'obligation posée par l'article 32 du Règlement.

***Perspectives** : L'autorité rappelle que des mesures de sécurité insuffisantes peuvent constituer un manquement à l'obligation de sécurité des données, sans qu'il soit nécessaire qu'une violation de données soit intervenue. Elle spécifie par ailleurs la portée de ses référentiels et guides, non obligatoires, mais servant de référence à ce qu'est « l'état de l'art », auquel sont comparées les mesures de sécurité mises en place par les responsables de traitement.*

SOURCE

28 décembre 2021 – Information en cas de violation, sécurité des données : sanction de 180 000 euros à l'encontre de la société SLIMPAY[4]

Par une décision en date du 28 décembre 2021, la CNIL a considéré que la société SLIMPAY avait manqué aux obligations suivantes posées par le RGPD :

- Manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués par un sous-traitant, en ce que certains contrats avec des sous-traitants ne contenaient aucune des mentions (ou certaines manquaient) prévues à l'article 28-3 du RGPD ;
- Manquement à l'obligation d'assurer la sécurité des données en ce que l'accès au serveur contenant des données d'état civil, des adresses postales et électroniques, les numéros de téléphone et des informations bancaires (BIC/IBAN) de plus de douze millions de personnes ne faisait l'objet d'aucune mesure de sécurité ;

[4] Délibération SAN-2021-020 du 28 décembre 2021.

- Manquement à l'obligation d'information d'une violation de données prévue à l'article 34 du RGPD en présence d'un risque élevé pour les personnes concernées ; risque considéré par la CNIL comme avéré au regard de la nature des données (bancaires notamment), du volume de personnes concernées (douze millions) et des risques pour les personnes concernées (usurpation d'identité, hameçonnage).

> ***Perspectives*** *: L'autorité rappelle également dans cette délibération que l'absence de preuve d'une utilisation frauduleuse des données est sans incidence sur la caractérisation du manquement à l'obligation de sécurité.*

SOURCE

II. Et en Europe ?

13 décembre 2021 - Sanction de 6,5 millions d'euros infligée à GRINDR par l'autorité de contrôle norvégienne

La société américaine GRINDR Inc. (ci-après « GRINDR ») commercialise une application de rencontre à destination de la communauté LGBTIQ+. Plusieurs plaintes relatives à des manquements à la réglementation en matière de données à caractère personnel ont été déposées en Europe, notamment par l'association NOYB. L'autorité administrative de contrôle norvégienne (Datatilsynet) avait notifié à GRINDR, le 24 janvier 2021, un projet de sanction à son encontre.

Le 13 décembre 2021, la sanction définitive a été prise par l'autorité norvégienne : la société a été condamnée pour traitements réalisés sans base légale (violation de l'article 6 RGPD) et traitement de données sensibles sans base légale adéquate ou exemption de celle-ci (violation de l'article 9 RGPD).

L'autorité a en effet considéré que le consentement obtenu – seule base légale envisageable pour l'autorité s'agissant de la publicité comportementale en ligne – n'était pas valide. Il ne permettait donc pas à la société de partager des données à des tiers, pour des finalités de publicité comportementale.

Dès lors que le consentement obtenu n'était pas valide, celui-ci ne pouvait pas justifier le traitement (et le partage à des tiers) des données sensibles au sens de l'article 9 du RGPD. En l'espèce, l'autorité considère en effet que l'utilisation de l'application GRINDR est une donnée relative à l'orientation sexuelle. Elle ajoute que l'article 9 doit être interprété largement et ne porte pas sur la révélation spécifique d'une orientation sexuelle.

Par ailleurs, le partage des données de localisation par GRINDR participe également, selon l'autorité, à l'illicéité du partage à un nombre conséquent de tiers des données des utilisateurs de GRINDR.

Enfin, le caractère élevé de la sanction – plus de 4% du chiffre d'affaires de GRINDR – est justifié par l'autorité pour servir d'exemple aux acteurs digitaux dont le business model est fondé sur le partage de données à des fins de publicité comportementale.

> ***Perspectives*** *: Dans cette décision, une attention particulière est portée au caractère unique (et donc illicite) du consentement donné par les utilisateurs de la plateforme à plusieurs finalités ou opérations de traitements ainsi qu'aux 'nudges' influant sur le choix des consommateurs. Les responsables de traitements doivent donc continuer à prêter attention à l'effectivité du contrôle et du choix des personnes concernées. Cette décision*

est également un rappel important que les sanctions administratives peuvent aller bien au-delà de 4% du chiffre d'affaires des sociétés, pour l'ensemble des acteurs et plus particulièrement pour les plateformes digitales pratiquant des transferts de données à des tiers aux fins de publicité comportementale ou conditionnant l'accès à leurs services à l'acceptation de partage de données à caractère personnel à de telles fins.

SOURCE

21 décembre 2021 – Réparation civile du préjudice découlant d'une violation du RGPD (tribunal civil allemand)

Le 21 décembre 2021, un tribunal civil allemand a accordé des dommages et intérêts sur le fondement de l'article 82 du RGPD. Aux termes de cet article, toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement a le droit d'obtenir du responsable de traitement ou du sous-traitant réparation du préjudice subi.

Dans cette décision, 2.500 euros ont été accordés pour réparation du préjudice moral à une victime d'une violation de données à caractère personnel ayant eu pour conséquence le vol de données relatives à son identité et ses finances.

Le responsable de traitement est par ailleurs également condamné pour tout préjudice matériel ultérieur. 33.000 personnes étaient concernées par la violation.

Perspectives *: Cette décision est intéressante, en ce qu'elle alimente la jurisprudence (quasiment inexistante) sur la réparation civile des dommages résultants des violations du RGPD. On peut s'interroger sur les conséquences de cette jurisprudence naissance, tant sur la publication des sanctions par les autorités de contrôle européennes (une autorité choisira-t-elle de publier une décision afin de favoriser une action civile des personnes concernées ?), que sur les pratiques des sociétés, s'agissant d'éventuels protocoles transactionnels suite à des violations de données.*

SOURCE

17 décembre 2021 – Décision d'adéquation de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par la République de Corée.

Après la conclusion des pourparlers d'adéquation en mars 2021, la décision d'adéquation pour le transfert de données à caractère personnel de l'Union européenne vers la République de Corée en vertu du RGPD a été adoptée.

Sur la base de cette décision, les données à caractère personnel pourront circuler en toute sécurité de l'Union européenne vers la République de Corée, au bénéfice des citoyens et des économies des deux parties, sans qu'il soit nécessaire d'obtenir d'autres autorisations ou de recourir à des outils supplémentaires.

La Commission a adopté la décision d'adéquation le 17 décembre 2021. Elle est applicable à compter du même jour.

***À retenir** : les transferts de données à caractère personnel depuis l'Union européenne vers la République de Corée peuvent être mis en œuvre sans garanties ou condition supplémentaires.*

SOURCE

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