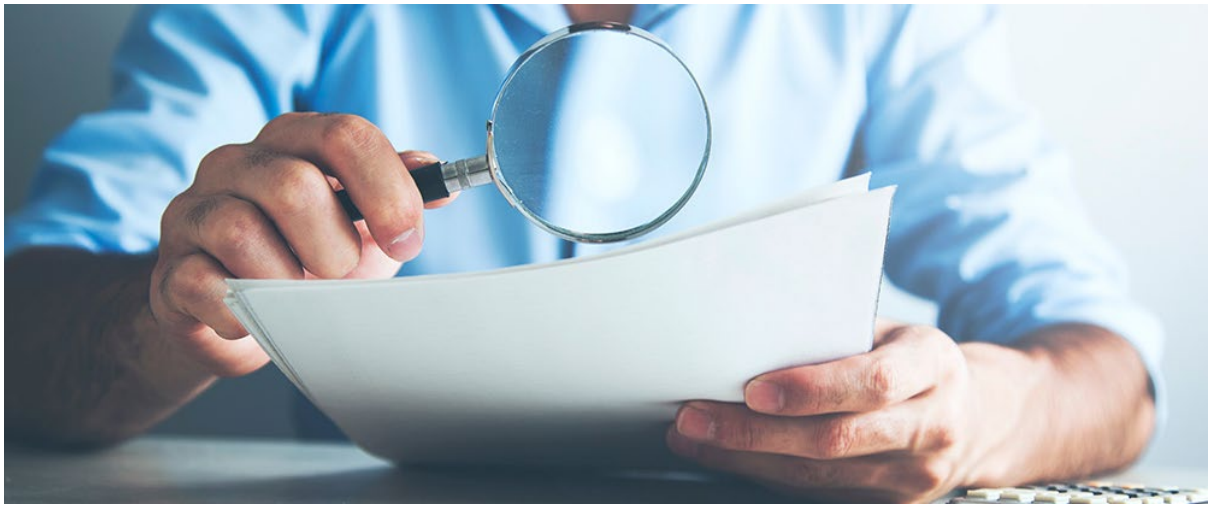
La Newsletter RGPD par @DerriennicParis

DERRIENNIC ASSOCIÉS

#NewsDerriennicRGPD 28



Madame, Monsieur,

La CNIL a fait preuve d'une certaine sévérité en cette fin d'année, en prononçant des sanctions particulièrement lourdes. La présente lettre d'informations leur sera principalement consacrée, au travers des sujets suivants :

- Plus de 3.000.000 € d'amendes prononcés par la CNIL à l'encontre de sociétés du groupe Carrefour ;
- Google et Amazon lourdement sanctionnés par la CNIL ;
- Deux médecins sanctionnés par la CNIL.

Ces décisions doivent nous encourager à garder le cap dans nos chantiers de mise en conformité au RGPD.

Par ailleurs, il est à noter que la CNIL a actualisé sa fiche pratique sur le droit d'accès.

Nous vous souhaitons une bonne lecture de la présente lettre et vous présentons nos meilleurs vœux pour 2021.

Formation à la préparation à la certification «DPO».

Le cabinet organise régulièrement des programmes de formation visant à la préparation des apprenants à l'examen de certification «DPO»

Retrouvez notre programme à la fin de notre newsletter.

Plus de 3.000.000 € d'amendes prononcés par la CNIL à l'encontre de sociétés du groupe Carrefour

La CNIL, saisie de plusieurs plaintes, a prononcé, le 18 novembre 2020, deux sanctions : l'une de 2.250.000 à l'encontre de Carrefour France et l'autre, de 800.000 euros, à l'encontre de Carrefour Banque.

Saisie de plusieurs plaintes ciblant des sociétés du groupe Carrefour, la CNIL a réalisé des contrôles auprès de Carrefour France et Carrefour Banque, au cours desquels elle a constaté un certain nombre de manquements.

1. La CNIL a relevé que l'information délivrée aux utilisateurs des sites carrefour.fr et carrefour-banque.fr n'était pas facilement accessible (notamment, un lien vers la politique de protection des données ne figurait pas systématiquement sur les formulaires de collecte), que les documents en question étaient longs et que leur contenu n'était pas exclusivement dédié à la protection des données.

Certaines formulations ont également été jugées inutilement compliquées, d'autres, rédigées en des termes généraux et imprécis, nuisaient à la compréhension du document. Par ailleurs, la durée de conservation des données n'était pas précisée.

La CNIL a estimé qu'il s'agissait là de manquements à l'obligation d'information de l'article 13 du RGPD.

2. La CNIL a constaté, par ailleurs que des cookies publicitaires étaient déposés sur le terminal des internautes se rendant sur les sites carrefour.fr et carrefour-banque.fr, dès la connexion à la page d'accueil du site, avant toute action de leur part, en violation de l'article 82 de la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés ».

3. Carrefour France demandait systématiquement la production d'un justificatif d'identité aux personnes souhaitant exercer leurs droits et n'était pas toujours en mesure de traiter ces demandes d'exercice des droits dans les délais prévus par le RGPD.

Cela a caractérisé, pour la CNIL, un manquement à l'article 12 du RGPD.

4. La CNIL a également relevé que Carrefour France n'avait pas donné suite à plusieurs demandes de droit d'accès émanant de personnes concernées.

Elle n'avait pas non plus donné suite à des demandes droit à l'effacement, dans des situations où elle était tenue de le faire, ni pris en compte des demandes d'opposition à la réception de publicité par SMS ou courrier électronique.

Ces éléments ont constitué, pour la CNIL, des manquements aux articles 15, 17 et 21 du RGPD.

5. Carrefour Banque communiquait à « Carrefour Fidélité » (qui était, en réalité, un service de Carrefour France) plus de données, concernant les personnes souscrivant à la carte de fidélité « Pass », que celles figurant dans la liste communiquée aux personnes concernées et présentée comme limitative.

Cela a constitué, pour la CNIL, un manquement à l'obligation de traiter les données de façon loyale, telle que formulée à l'article 5 du RGPD.

La CNIL, bien qu'elle ait relevé que l'ensemble des manquements identifiés avaient été corrigés par les sociétés du groupe Carrefour, a sanctionné Carrefour France d'une amende de 2.250.000 euros et Carrefour Banque d'une amende de 800.000 euros.

Lien vers la décision concernant Carrefour France :

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756

Lien vers la décision concernant Carrefour Banque :

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042564657

Google et Amazon lourdement sanctionnés par la CNIL

Par deux délibérations du 7 décembre 2020, la CNIL a condamné d'une part, les sociétés Google LLC et Google Ireland Limited à des amendes de 60 et 40 millions d'euros ; et, d'autre part, la société Amazon Europe Core à une amende de 35 millions d'euros. Ces sanctions sont motivées par des manquements à la législation applicable en matière de cookies..

1. Au cours de contrôles en ligne menés en 2020 sur les sites google.fr et amazon.fr, la CNIL a constaté un certain nombre de manquements à l'article 82 de la loi « Informatique et libertés » du 6 janvier 1978 modifiée. Cet article impose au responsable du traitement d'informer et de recueillir le consentement de l'internaute préalablement à l'utilisation de cookies.

La CNIL a, tout d'abord, relevé que des cookies à finalité publicitaire étaient déposés sur le terminal des internautes se rendant sur les sites amazon.fr et google.fr, et ce dès leur arrivée sur ces sites, avant toute action de leur part, fût-ce une simple poursuite de la navigation, qui aurait pu, à l'époque, être admise comme modalité valable d'expression du consentement.

La CNIL a ensuite souligné qu'aucune information n'était délivrée aux internautes sur le site google.fr. Sur le site amazon.fr, si un bandeau d'information indiquait bien la présence de cookies avec pour finalité « *offrir et améliorer nos services* », le CNIL a jugé cette formulation comme une description « *générale et approximative des finalités de l'ensemble des cookies* », qui n'était pas de nature à satisfaire à l'obligation d'information de l'article 82.

Enfin, la CNIL a constaté qu'après avoir désactivé la personnalisation des annonces sur la recherche Google, des cookies à finalités publicitaires demeuraient néanmoins stockés sur son équipement terminal.

2. Tirant les conséquences de ces manquements, la CNIL a prononcé les amendes administratives suivantes :

- 60 millions d'euros à l'encontre de la société Google LLC ;
- 40 millions d'euros à l'encontre de la société Google Ireland Limited ;
- 35 millions d'euros à l'encontre de la société Amazon Europe Core.

Ces amendes s'accompagnent d'injonctions de correction des manquements, assorties d'astreintes de 100.000 euros par jour de retard.

Il s'agit là de sanctions particulièrement lourdes, parmi les plus sévères prononcées par une autorité de contrôle européenne, et dont il est à noter qu'elles ne résultent pas de manquements au RGPD.

Notons également qu'avant 2017, ce type de manquement pouvait faire l'objet d'une amende administrative d'un montant maximum de 150.000 €. La loi pour une République numérique a ensuite porté ce montant à un maximum de 3 millions d'euros. Depuis l'ordonnance du 12 décembre 2018, les manquements à la loi « Informatique et libertés » peuvent entrainer le prononcé d'amendes dont le montant peut aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial, voire, dans certains cas, 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

Il convient de relever que, depuis les faits, les obligations pesant sur les entités utilisant des cookies se sont renforcées. En effet, il désormais nécessaire pour éditeur d'un site web, responsable du traitement, de recueillir un consentement répondant aux exigences du RGPD, lequel ne saurait être déduit d'une simple poursuite de la navigation de l'utilisateur.

Liens vers les publications de la CNIL :

https://www.cnil.fr/fr/cookies-sanction-de-35-millions-deuros-lencontre-damazon-europe-core

https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-google-llc-et-de-40-millions-deuros-lencontre-de

Liens vers les délibérations :

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706

Deux médecins sanctionnés par la CNIL

Par deux décisions du 7 décembre 2020, la formation restreinte de la CNIL a prononcé deux amendes (3.000 et 6.000 euros) à l'encontre de deux médecins libéraux en raison notamment d'un manquement à leur obligation de sécurité des données.

Dans le cadre d'un contrôle en ligne, la CNIL a constaté que des milliers d'images médicales (IRM, radios, scanners, etc.), suivies notamment des noms, prénoms, date de naissance et date de consultation des patients, étaient librement accessibles sur internet.

Il ressort de ces investigations que la violation de données avait pour cause « l'ouverture des ports réseaux de la box internet (…) couplée au paramétrage de la fonction serveur du logiciel d'imagerie » de ces médecins.

La CNIL a considéré qu'il s'agissait, pour ces deux professionnels de santé, d'un manquement à l'obligation d'assurer la sécurité des données, dès lors que la protection du réseau informatique et le chiffrement des données font partie des exigences élémentaires en matière de sécurité informatique.

La CNIL a également relevé que les médecins n'avaient pas pris le soin de chiffrer les données contenues dans leurs ordinateurs fixes et portables. « Or, en l'absence de chiffrement, précise la CNIL, les données médicales contenues dans le disque dur de ces ordinateurs étaient lisibles en clair par toute personne prenant possession de ces appareils (par exemple, à la suite de leur perte ou de leur vol) ou par toute personne s'introduisant de manière indue sur le réseau auquel ces appareils étaient raccordés. »

La CNIL a par ailleurs retenu un manquement à l'obligation de notifier les violations de données, notification qui aurait dû être effectuée après qu'ils aient appris l'existence d'une telle violation, la CNIL précisant que « la circonstance que la violation de données avait été portée à [leur] connaissance par le service des contrôles de la CNIL ne [les] déchargeait pas de cette obligation ».

En conclusion la CNIL souligne que : « Si la formation restreinte n'a pas considéré nécessaire que l'identité des médecins concernés soit rendue publique, elle a néanmoins souhaité assurer la publicité de ces décisions pour alerter les professionnels de la santé sur leurs obligations et la nécessité de renforcer leur vigilance sur les mesures de sécurité apportées aux données personnelles qu'ils traitent. Cette vigilance doit les conduire à choisir les solutions applicatives présentant le maximum de garanties en termes de sécurité informatique et de protection des données personnelles. Elle doit également les inciter à la prudence au moment de l'élaboration et du paramétrage de leur système informatique interne, en s'entourant si nécessaire de prestataires compétents en la matière. »

La CNIL actualise sa fiche pratique sur le droit d'accès

Le 18 novembre dernier, la CNIL a actualisé sa fiche pratique relative aux modalités de réponse à une demande de droit d'accès d'une personne concernée.

Pour mémoire, le RGPD et la loi Informatique et Libertés permettent à toute personne d'accéder aux données qui la concernent.

Il en ressort que la personne concernée peut demander l'accès à l'information sur le traitement éventuel de données la concernant ainsi que l'obtention d'une copie de ces données.

A ce titre, la CNIL rappelle que toute personne peut exercer son droit d'accès auprès d'un organisme, dès l'instant qu'il détient des données personnelles la concernant. Par exemple, peuvent être destinataires d'une demande d'accès : la société dont la personne est cliente, son employeur, son médecin ou encore, une administration.

Face à une telle demande, l'organisme doit mettre en œuvre une procédure interne adaptée afin d'apporter une réponse conforme au RGPD et à la loi Informatique et Libertés.

Dans cette perspective, la fiche pratique publiée par la CNIL (accessible ici) a vocation à rappeler aux professionnels les bonnes pratiques à adopter pour répondre correctement à une demande d'exercice de droit d'accès.

1. Démarche à adopter face à une demande d'exercice de droit d'accès

La CNIL recommande aux organismes destinataires d'une demande d'exercice de droit d'accès de suivre les quatre étapes suivantes :

(i) Tout d'abord, en cas de doute, l'organisme peut **vérifier l'identité de la personne** qui exerce sa demande.

A ce titre, la CNIL rappelle que la justification de l'identité de la personne concernée peut intervenir « par tous moyens » (par exemple, par la fourniture d'un numéro client ou adhérent) et précise que la demande de la pièce d'identité de la personne ne doit intervenir qu'en cas de « doute raisonnable sur l'identité du demandeur ».

(ii) Ensuite, lorsque la demande porte sur une grande quantité de données, l'organisme peut demander à la personne concernée de **préciser sur quelles données ou quels traitements de données porte sa demande**.

(iii) L'organisme doit **respecter les droits des tiers**, ce qui implique qu'il doit :

- Vérifier que la demande ne concerne pas un tiers (par exemple, le conjoint ou le collègue de la personne), sauf à justifier d'un mandat en bonne et due forme ; et
- Veiller, dans la réponse, à ne pas porter atteinte aux droits des tiers, au secret des affaires ou à la propriété intellectuelle (par exemple, en masquant des éléments dans les documents transmis au demandeur).

(iv) Enfin, l'organisme doit **respecter les délais de réponse** imposés.

La CNIL rappelle que la réponse doit intervenir :

- En cas de demande simple : dans un délai d'un mois maximum à compter de la demande.
- En cas de demande portant sur des données de santé : dans un délai de quarante-huit heures minimum (compte tenu du délai de réflexion

légal) et de huit jours maximum suivant la demande.

A noter que si les données de santé sont traitées depuis plus de cinq ans, le délai de réponse est porté à deux mois.

- En cas de demande complexe (par exemple, portant sur un grand nombre de données) : dans un délai de 3 mois maximum à compter de la demande.

S'il est possible de refuser de faire droit à la demande de la personne (par exemple, lorsque la demande est infondée ou excessive ou encore, lorsque les données ont été effacées), la CNIL rappelle qu'il convient d'en informer le demandeur dans un délai d'un mois.

2. Précisions sur les obligations pesant sur les organismes

La CNIL rappelle que des obligations pèsent sur les organismes et apporte des précisions à cet égard. En particulier :

(i) Tout d'abord, la CNIL indique que l'organisme doit **prendre des mesures pratiques** permettant à la personne concernée d'exercer son droit d'accès (par exemple, par le biais d'un formulaire en ligne) et mettre en place une **procédure interne efficace** pour traiter la demande dans les délais impartis et répondre au demandeur de manière compréhensible, accessible et formulée en des termes clairs et simples.

(ii) La CNIL estime que les **données personnelles présentes dans un document** (par exemple, enregistrement vocal, courrier, rapport, etc.), peuvent être communiquées soit par la copie du document lui-même, soit par une retranscription fidèle sur un autre support.

Aussi, s'agissant des données personnelles enregistrées dans un « logiciel métier » (par exemple, CRM ou gestion RH), la CNIL précise qu'elles peuvent être communiquées par la transmission d'impressions d'écrans du logiciel métier ou par une retranscription fidèle sur tout autre support.

(iii) La CNIL recommande de **conserver une preuve de l'envoi et la réception de la réponse** apportée au demandeur (par exemple, en répondant par écrit à une demande écrite, en envoyant un courrier par LRAR).

(iv) Enfin, la CNIL impose aux organismes de **sécuriser la transmission des données**. A titre d'exemple, la CNIL propose de chiffrer les données qui seraient transmises par une clé USB afin d'éviter que ces données soient accessibles à tous.

DERRIENNIC ASSOCIES PROPOSE UN PROGRAMME DE FORMATION DE 35 HEURES POUR LA PRÉPARATION A LA CERTIFICATION DPO

OBJECTIF

1/ Acquérir les compétences, les connaissances et le savoir-faire attendus par la CNIL et permettre au collaborateur de se présenter à l'examen de certification en maximisant ses chances de succès.

2/ Indépendamment de la certification, la formation permet à l'apprenant de se familiariser avec la matière et d'acquérir les compétences, les connaissances et le savoir-faire pour :

- analyser une situation impliquant un traitement de données personnelles ;
- définir et appréhender les problématiques, les enjeux et les risques qui en découlent ;
- prendre les décisions qui s'imposent en concertation avec l'équipe « DPO »

CONTENU DE LA FORMATION

PARTIE 1 - Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité

PARTIE 2 - Responsabilité (Application du principe d'« Accountability »)

PARTIE 3 - Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

COÛT

3000€ HT/personne

INTERVENANT

ALEXANDRE FIEVEE
Avocat Associé
Tél : 01.47.03.14.94
afievee@derriennic.com

CLASSEMENTS

Alexandre Fievee figure dans le classement Best Lawyers dans la catégorie **« Information Technology Law » (2020).**

Il a également fait en **2020** son entrée dans le classement Legal 500 dans la catégorie **« Next Generation Partners »**.

RENSEIGNEMENTS PRATIQUES

PROCHAINE SESSION 2020/2021 :
Sur demande.

LIEU DE LA FORMATION :
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.

INSCRIPTION ET INFORMATIONS :
afievee@derriennic.com