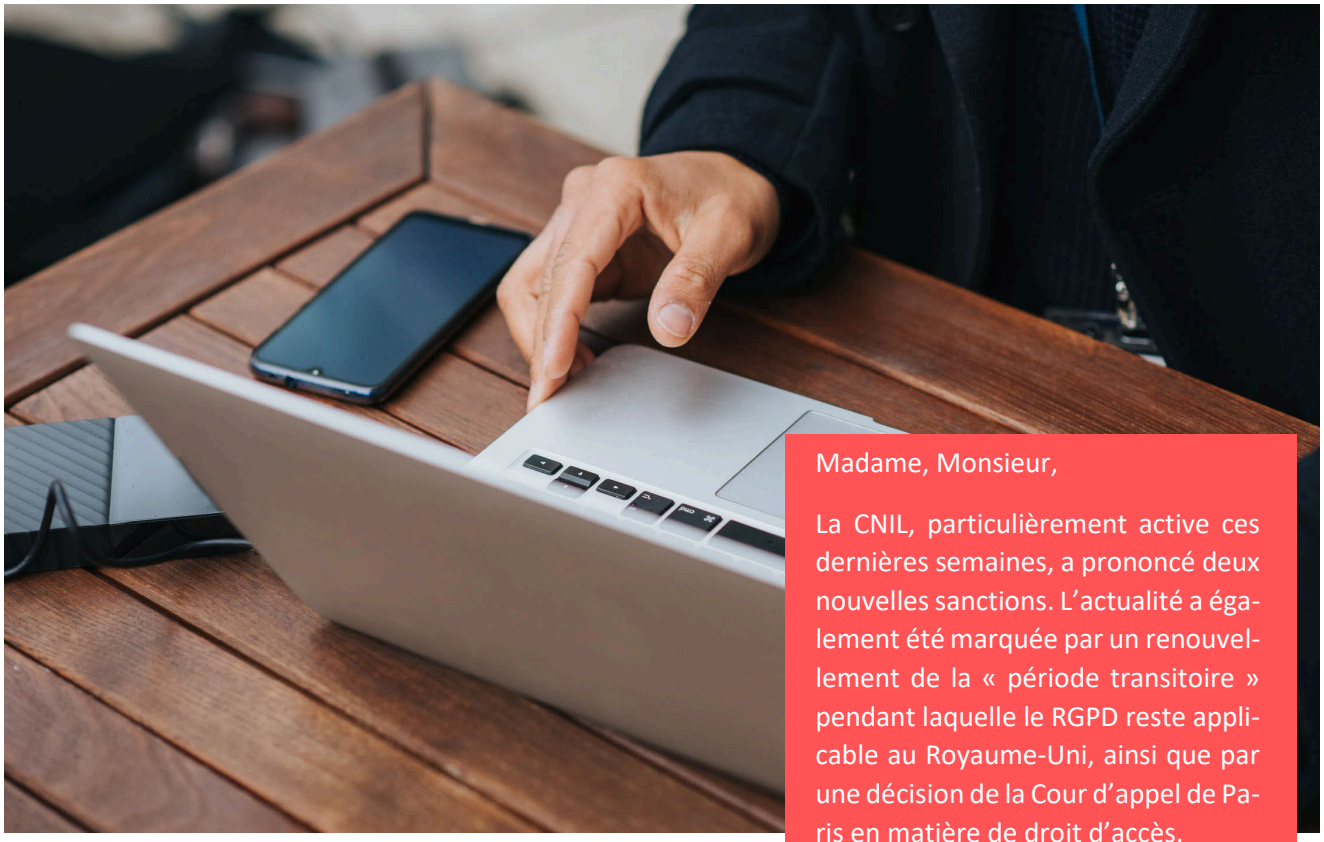
NEWSLETTER RGPD

NUMÉRO 29 • FÉVRIER 2021



Madame, Monsieur,

La CNIL, particulièrement active ces dernières semaines, a prononcé deux nouvelles sanctions. L'actualité a également été marquée par un renouvellement de la « période transitoire » pendant laquelle le RGPD reste applicable au Royaume-Uni, ainsi que par une décision de la Cour d'appel de Paris en matière de droit d'accès.

Nous vous proposons ainsi de découvrir les actualités suivantes :

ACTUALITE DU CABINET

FORMATION A LA PREPARATION A 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. **P9**

SOMMAIRE

PROSPECTION COMMERCIALE :

NESTOR CONDAMNEE PAR LA CNIL A UNE AMENDE DE 20.000 €

LA SOCIETE DE PREPARATION ET DE LIVRAISON DE REPAS NESTOR A ETE CONDAMNEE PAR LA CNIL, LE 8 DECEMBRE 2020, A UNE AMENDE DE 20.000€ NOTAMMENT POUR DEFAUT DE RECUEIL DU CONSENTEMENT PREALABLEMENT A L'ENVOI DE COURRIELS DE PROSPECTION.

En 2018, la CNIL a été saisie par des plaintes de personnes indiquant avoir reçu des courriels de prospection émanant de la société Nestor, sans jamais avoir consenti à ces opérations de prospection et sans être des clients de cette dernière. A l'occasion d'un contrôle en ligne, suivi d'un contrôle sur place, la CNIL a relevé que :

- la société Nestor constituait sa base de prospects à partir de données à caractère personnel accessibles en ligne sur un site web de réseau social professionnel ;
- la société Nestor ne recueillait pas le consentement des prospects conformément à l'article L 34-5 du Code des postes et des communications électroniques (CPCE) ;
- la société Nestor ne donnait pas suite aux demandes d'exercice de droit d'accès dont elle était saisie de façon satisfaisante et dans les délais prescrits pas le RGPD ;
- la société Nestor acceptait que le mot de passe des utilisateurs soient composés d'un seul caractère, en dépit de l'obligation de sécurité pesant sur celle.

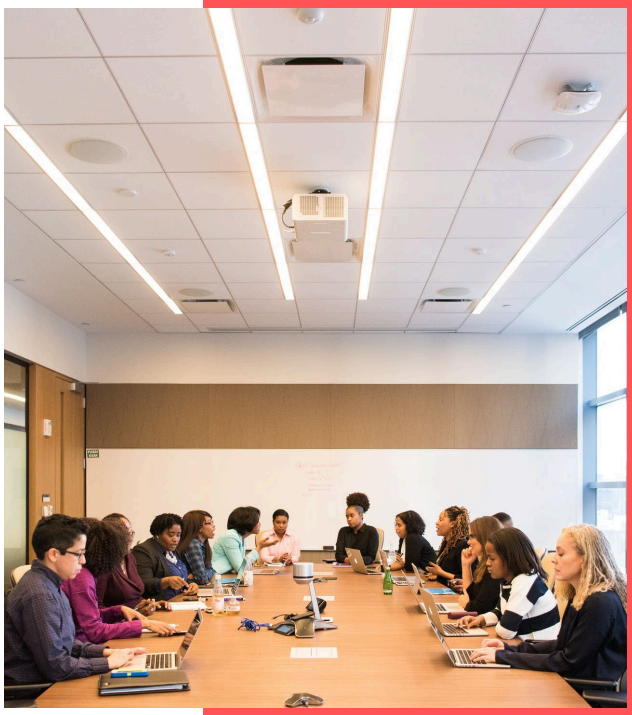
La CNIL a, en conséquence, prononcé une amende de 20.000 € à l'encontre de Nestor et l'a enjoint de mettre en conformité les traitements de données litigieux, sous astreinte de 500 € par jour de retard.

Lien vers la publication de la CNIL :

https://www.cnil.fr/fr/prospection-commerciale-sanction-de-20-000-euros-lencontre-de-la-societe-nestor

PROSPECTION COMMERCIALE :

LA CNIL CONDAMNE UNE AGENCE DE MARKETING A UNE AMENDE DE 7.300 €



PAR UNE DELIBERATION EN DATE DU 7 DECEMBRE 2020, LA CNIL A PRONONCE UNE AMENDE D'UN MONTANT DE 7.300 EUROS A L'ENCONTRE DE LA SOCIETE PERFORMECLIC EN RAISON DE MANQUEMENTS AU RGPD ET AU CODE DES POSTES ET DES COMMUNICATIONS ELECTRONIQUES (« CPCE »).

La société PERFORMECLIC est une petite entreprise ayant pour activité l'envoi de prospection commerciale par courriers électroniques pour le compte d'annonceurs. Elle détient, à cette fin, une base de données de plus de 20 millions d'adresses électroniques de prospects.

Le 12 juin 2019, la CNIL a été alertée des pratiques de la société PERFORMECLIC par l'association SIGNAL SPAM, en charge de recueillir les signalements des internautes relatifs à la réception de courriers électroniques non sollicités (« SPAM »).

Dans son signalement, l'association indiquait que la société PERFORMECLIC apparaissait régulièrement en tête du classement des sociétés émettant le plus de messages signalés comme « SPAM » par les internautes français (163.000 signalements recensés entre le 1er janvier et le 11 juin 2019).

A l'issue d'un contrôle sur place puis d'une audition, la CNIL a, après avoir qualifié la société PERFORMECLIC de responsable du traitement au sens du RGPD, retenu plusieurs manquements.

1/ Sur la qualification de responsable du traitement

La CNIL a estimé qu'il ressort d'un « faisceau d'indices concordants » que la société PERFORMECLIC est responsable du traitement lié à la gestion et la mise à disposition de sa base de données pour l'envoi de campagnes publicitaires à des prospects par courrier électronique pour le compte d'annonceurs.

Tout d'abord, il ressort des échanges intervenus entre la CNIL et la société PERFORMECLIC que cette dernière indiquait explicitement être responsable du traitement.

Selon la CNIL, plusieurs éléments confirmaient cette qualification :

- En premier lieu, la CNIL a estimé que la société PERFORMECLIC détermine les finalités du traitement puisque «la mise à disposition de sa base de prospects à des fins de prospection commerciale est au cœur de l'activité de la société » et que cette dernière est « propriétaire de la base de données utilisée dans le cadre des campagnes de prospection» ;

- En second lieu, la CNIL a considéré que la société PERFORMECLIC détermine les moyens essentiels du traitement en ce qu'elle « définit les données personnelles qui figurent dans sa base de prospects, les durées pendant lesquelles ces données y sont conservées et les éventuelles mises à jour devant être opérées ».

En conséquence, la CNIL a qualifié la société PERFORMECLIC de responsable du traitement « sans qu'il soit nécessaire de se prononcer sur une éventuelle responsabilité conjointe des partenaires annonceurs de la société PERFORMECLIC ».

2/ Sur les manquements au RGPD et au CPCE

La CNIL a retenu un manquement au CPCE et cinq manquements au RGPD :

- Tout d'abord, la CNIL a relevé un manquement de la société PERFORMECLIC à son obligation de recueillir le consentement de la personne concernée par une opération de prospection directe au moyen d'un courrier électronique (art.L.34-5 du CPCE). En effet, la CNIL a considéré que la société ne disposait d'aucun élément permettant de matérialiser le recueil effectif du consentement des prospects à l'envoi de prospection commerciale, que ce soit par elle-même ou par la société qui lui avait vendu la base de données.

- La CNIL a relevé un manquement de la société PERFORMECLIC à son obligation de minimisation des données (art. 5.1.c du RGPD), compte tenu de la présence du numéro de téléphone sur les fiches des prospects alors qu'il n'est pas utilisé dans le cadre de l'envoi des courriers électroniques.

- Aussi, la CNIL a estimé que la société PERFORMECLIC conservait les données pendant une durée excessive (art. 5.1.e du RGPD). En effet, la société conservait plus de trois ans les coordonnées d'environ 5 millions de prospects ayant uniquement ouvert les courriels de prospection, sans autre action de leur part, ce qui «ne saurait être [suffisant] pour matérialiser [leur] intérêt effectif».

  A ce titre, la CNIL a rappelé qu'elle recommande dans sa norme dédiée (NS-048, accessible ici) «que les données à caractère personnel relatives à un prospect non client soient conservées pendant un délai de trois ans à compter du dernier contact émanant du prospect, matérialisé par exemple par un clic sur un lien hypertexte contenu dans un courrier électronique».

- La CNIL a également considéré que la société PERFORMECLIC avait manqué à son obligation d'information des personnes concernées en ne communiquant pas toutes les informations requises par l'article 14 du RGPD, à savoir : « l'identité du responsable de traitement, sa base juridique, les catégories de données personnelles concernées, la durée de conservation des données, l'ensemble des droits des personnes (en particulier le droit à la portabilité et le droit à la limitation du traitement), le droit d'introduire une réclamation auprès d'une autorité de contrôle et la source d'où proviennent les données ».

- En outre, la CNIL a considéré que le droit d'opposition des personnes concernées (art. 21 du RGPD) n'était pas pris en compte de manière effective puisque «lorsqu'une personne clique sur un lien de désabonnement pour exercer son droit d'opposition, celle-ci est désabonnée du compte utilisé pour l'envoi de la campagne de prospection concernée mais pas des autres comptes utilisés par la société pour d'autres campagnes». De plus, la CNIL a relevé que les personnes concernées n'étaient pas informées de la marche à suivre pour être désinscrites de l'ensemble des comptes utilisés pour l'envoi de courriels de prospection par la société PERFORMECLIC.

- Enfin, la CNIL a estimé que la société PERFORMECLIC avait manqué à son obligation d'encadrer contractuellement ses relations avec son sous-traitant (art. 28 du RGPD), lequel était en charge de la diffusion technique des courriels, de l'hébergement de sa base de données et du traitement des campagnes publicitaires des annonceurs. En effet, la CNIL a relevé que certaines clauses requises par l'article 28 du RGPD ne figuraient pas dans le contrat puisque « le contrat conclu entre la société et son sous-traitant ne contenait pas de clauses prévoyant que le sous-traitant :

    - Veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
    - Met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ».

Compte tenu de ces manquements, la CNIL a prononcé une amende administrative d'un montant de 7.300 euros et a enjoint la société de se mettre en conformité dans un délai de 2 mois. A défaut de mise en conformité dans ce délai, la société s'exposera au paiement d'une astreinte de 1 000 euros par jour de retard.

Lien vers la délibération :

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042774286?isSuggest=true

TRANSFERT DE DONNEES :

BREXIT : LE STATU QUO

LA CNIL AVAIT PUBLIE, LE 31 JANVIER 2020, JOUR DE LA SORTIE DU ROYAUME-UNI DE L'UNION EUROPEENNE, UN TEXTE INDIQUANT QU'EN APPLICATION DE L'ACCORD DE RETRAIT, LES DISPOSITIONS DU RGPD CONTINUERAIENT A S'APPLIQUER A CE PAYS PENDANT UNE PERIODE TRANSITOIRE COURANT JUSQU'AU 31 DECEMBRE 2020. LA CNIL INDIQUAIT QUE CETTE PERIODE TRANSITOIRE POURRAIT FAIRE L'OBJET D'UNE PROLONGATION.

C'est chose faite.

Le 24 décembre 2020, le Royaume-Uni et l'Union européenne ont convenu, dans le cadre de l'accord de commerce et de coopération, que le RGPD restera applicable au Royaume-Uni pour une durée de 6 mois supplémentaires.

Une nouvelle période transitoire s'ouvre donc, pendant laquelle les transferts de données personnelles vers le Royaume-Uni continueront à se faire comme si le pays destinataire était un pays de l'Union européenne et non un pays tiers.

« A l'issue de cette période de 6 mois et à défaut d'une décision de la Commission européenne autorisant de façon générale les transferts de données personnelles vers le Royaume-Uni dite « décision d'adéquation », toute communication de données personnelles vers le Royaume-Uni sera considérée comme un transfert de données vers un pays tiers.

De tels transferts ne pourront s'effectuer qu'avec la mise en place de garanties appropriées, telles que prévues par le RGPD (ex : clauses contractuelles types, règles contraignantes d'entreprise, etc.) et à la condition que les Européens disposent de droits opposables et de voies de droit effectives, conformément à l'article 46 du RGPD », précise la CNIL.

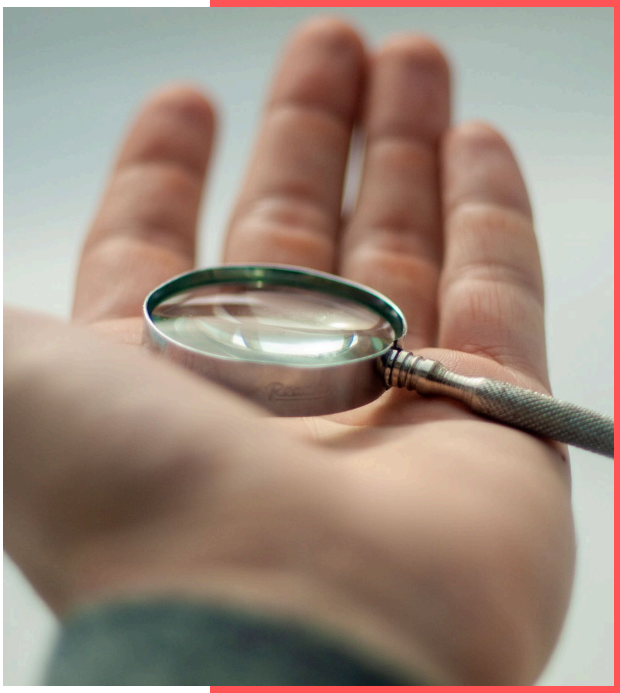
Il convient toutefois de préciser que la mise en place de telles garanties pourrait ne pas s'imposer, dans le cas où la Commission européenne adopterait, d'ici le 1er juillet 2021, une décision reconnaissant que le Royaume-Uni garantit un niveau de protection adéquat.

Lien vers la publication de la CNIL :

https://www.cnil.fr/fr/brexit-le-rgpd-reste-applicable-au-royaume-uni-jusquau-1er-juin-2021

DROIT D'ACCES :

LA COUR D'APPEL DE PARIS ENJOINT L'EMPLOYEUR DE REMETTRE, SOUS ASTREINTE, L'INTEGRALITE DE SES DONNEES PERSONNELLES AU SALARIE



DANS UN ARRET RENDU LE 29 OCTOBRE DERNIER, LA COUR D'APPEL DE PARIS S'EST PRONONCEE SUR UNE DEMANDE D'EXERCICE DE SON DROIT D'ACCES FORMULEE PAR UNE SALARIEE AUPRES DE SON EMPLOYEUR.

Dans les jours qui ont suivi la notification de son licenciement pour faute grave, une salariée a adressé un courrier à son employeur aux termes duquel non seulement elle contestait les motifs de son licenciement, mais également elle sollicitait la restitution de ses données personnelles.

N'ayant pas obtenu de son employeur une telle restitution, la salariée a demandé au Conseil des prud'hommes puis à la Cour d'appel de Paris de condamner son employeur notamment à lui remettre l'intégralité de ses données personnelles.

L'employeur invoquait le fait que les données étant quérables, il appartenait à la salarié de venir les récupérer avec une clé USB.

Or, la salarié, qui a pu récupérer certains effets personnels à l'occasion d'un rendez-vous dans les locaux de l'entreprise, n'a pas, selon l'employeur, profité de cette visite pour récupérer ses données.

Cette version des faits était contestée par la salarié qui affirmait n'avoir pas pu, ce jour-là, pénétrer dans les locaux de l'entreprise.

Selon la Cour d'appel de Paris, l'employeur n'était pas légitime à opposer le caractère quérable des données, pour les raisons suivantes :

«Si comme le soutient [l'employeur], les données personnelles de la salariée sont en principe quérables, le rendez-vous à cet effet dans les locaux de l'entreprise doit être organisé loyalement et en temps utile, le salarié ne devant pas être confronté à une opposition de fait ni à une quelconque réticence de l'employeur.

Or, à la date du 14 octobre 2019, la remise ou la récupération des données personnelles contenues dans l'ordinateur professionnel de la salariée était déjà en question depuis plusieurs mois, de sorte qu'il est manifeste que celle-ci n'a pas été en mesure, à l'occasion du rendez-vous convenu, de récupérer ses données personnelles.

Dans ces conditions, [l'employeur] n'est plus fondé à opposer le caractère quérable desdites donnée.»

Par conséquent, la Cour d'appel de Paris a infirmé l'ordonnance et a enjoint l'employeur de « remettre » à la salariée « l'intégralité de ses données personnelles sur un support et dans un langage exploitables » et ce, dans un délai de trente jours à compter de la signification de l'arrêt, sous peine ensuite d'une astreinte de 50 euros par jour de retard pendant 6 mois.

Références de la décision :

CA Paris 29 oct. 2020 n°19/11748

ACTUALITE DU CABINET

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

COUT

3000€ HT/personne

INTERVENANT

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

Classements
Alexandre Fievee figure dans le classement BestLawyers 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