La Newsletter dédiée à la mise en conformité au RGPD

par @DerriennicParis

DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 26

Madame, Monsieur,

La rentrée a été marquée par plusieurs actualités d'intérêt, notamment la publication, par le CEPD, de lignes directrices riches en informations sur la relation entre responsable du traitement et sous-traitant. La CNIL a également rendu plusieurs délibérations en matière de cookies. Nous vous proposons donc, en ce mois d'octobre 2020, de découvrir les articles suivants :

- Une nouvelle loi encadrant les démarchages téléphoniques ;
- Cookies : La CNIL confirme ses positions ;
- Lignes directrices du CEPD : Comment rédiger son contrat de sous-traitance ? ;
- Manquements multiples dans le traitement de données clients : 250.000€ d'amende ;
- COVID-19 : Quelle collecte des données par l'employeur ?
- L'autorité de protection des données d'Hambourg prononce une sanction pécuniaire record de 35,3 millions d'euros

Nous vous en souhaitons une bonne lecture.

Une nouvelle loi encadrant les démarchages téléphoniques

Une loi visant à encadrer les démarchages téléphoniques et lutter contre les appels frauduleux a été promulguée le 24 juillet 2020.

Une nouvelle loi sur le démarchage téléphonique a été publiée le 25 juillet 2020, avec pour objet d'encadrer les démarchages et de lutter contre les appels frauduleux.

1. Cette loi introduit l'obligation, pour les fournisseurs de services de communications électroniques, d'inclure dans les contrats conclus avec les consommateurs, une mention les informant de leur faculté de s'inscrire gratuitement sur la liste d'opposition au démarchage téléphonique (liste « Bloctel » interdisant aux professionnels de démarcher les consommateurs qui y sont inscrits).

Cette faculté doit désormais également être communiquée par tout professionnel contactant un consommateur par téléphone en vue de la conclusion d'un contrat de vente ou de fourniture de service.

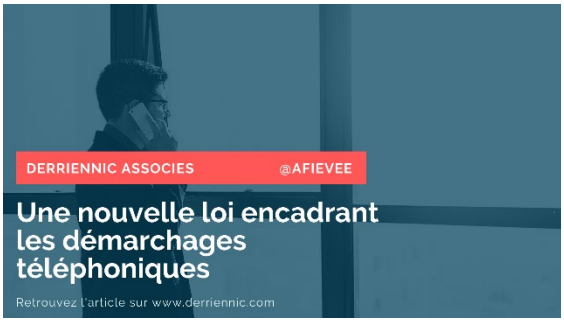
2. De plus, cette loi interdit purement et simplement la prospection à destination des consommateurs, par voie téléphonique, ayant pour objet la vente d'équipements ou la réalisation de travaux pour des logements en vue de la réalisation d'économies d'énergie.

3. Certaines activités de démarchage (notamment la sollicitation d'un consommateur inscrit sur la liste d'opposition au démarchage téléphonique, lorsqu'elle intervient dans le cadre de l'exécution d'un contrat en cours et a un rapport avec l'objet de ce contrat) sont maintenant interdites en dehors de jours et d'horaires qui restent à déterminer par décret.

4. Ces nouvelles dispositions viennent compléter le cadre juridique préexistant en matière de démarchage téléphonique, à l'instar de l'article L221-17 du Code de la consommation, qui interdit l'utilisation d'un numéro masqué dans le cadre d'opérations de démarchage.

Elles s'accompagnent d'un rehaussement général du montant des amendes pouvant être prononcées en cas de violation d'une des dispositions relatives au démarchage, qui peuvent désormais atteindre 75.000€ (précédemment : 3.000€ et, pour certaines infractions, 15.000€) pour une personne physique et 375.000€ (précédemment : 15.000€ et, pour certaines infractions, 75.000€) pour une personne morale.

Lien vers la loi n° 2020-901 du 24 juillet 2020 : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000042148119&categorieLien=id#:~:text=LOI%20n%C2%B0%202020%2D901,contre%20les%20appels%20frauduleux%20%7C%20Legifrance



Cookies : La CNIL confirme ses positions

Par deux délibérations du 17 septembre 2020, la CNIL a adopté, d'une part, de nouvelles lignes directrices relatives à l'utilisation des cookies et, d'autre part, la version définitive de ses recommandations visant à proposer des modalités pratiques de recueil d'un consentement conforme aux règles applicables.

1. En 2013, la CNIL avait adopté une première recommandation pour guider les acteurs dans la mise en œuvre des textes régissant les opérations de lecture et d'écritures par des cookies. Elle y avait indiqué que le consentement de l'utilisateur pouvait se déduire de la poursuite de sa navigation sur le site.

Le 25 mai 2018, l'entrée en application du RGPD a renforcé les exigences en matière de validité du consentement, rendant obsolète une partie de cette recommandation. En effet, selon le RGPD, le consentement doit être libre, éclairé, spécifique et univoque. Il ne saurait résulter que d'un acte positif clair, et ne peut plus être déduit de la simple poursuite de la navigation, sur le site, par l'internaute.

2. La CNIL a, en conséquence, entrepris d'actualiser ses cadres de référence pour les adapter à ces nouvelles règles.

Elle a ainsi adopté, le 4 juillet 2019, des lignes directrices rappelant le droit applicable, qui ont fait l'objet d'un ajustement le 17 septembre 2020 afin de tirer les conséquences d'une décision du Conseil d'Etat rendue le 19 juin 2020.

Elle a également lancé un projet de recommandation, dont la version finale a été adoptée le 17 septembre 2020, et dont l'objet est de proposer des modalité pratiques de recueil d'un consentement conforme au RGPD.

Les lignes directrices sont accessibles à l'adresse url suivante : https://www.cnil.fr/sites/default/files/atoms/files/ligne-directrice-cookies-et-autres-traceurs.pdf

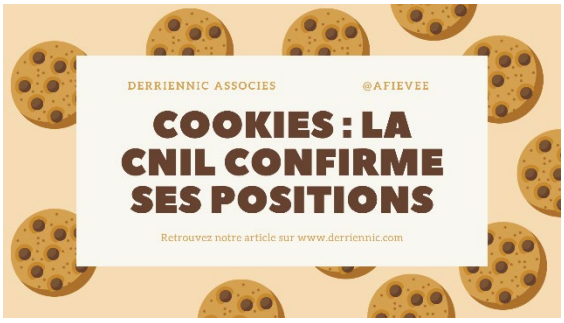
La recommandation de la CNIL est accessible à l'adresse url suivante : https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf

3. Par ailleurs, la CNIL est venue préciser que si elle va continuer à veiller au respect, par les opérateurs, des règles applicables en matière de consentement, elle ne sanctionnera les manquements au nouveau cadre juridique posé par sa recommandation et ses lignes directrices qu'à l'issue d'une « *période d'adaptation* » de 6 mois.

Les opérateurs ont donc jusqu'au 1er avril pour se mettre en conformité avec le nouveau cadre règlementaire.

Lien vers la publication de la CNIL : https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation

Lien vers la FAQ de la CNIL sur les lignes directrices et sa recommandation : https://www.cnil.fr/fr/questions-reponses-sur-les-lignes-directrices-modificatives-et-la-recommandation-cookies-et-autres



Lignes directrices du CEPD : Comment rédiger son contrat de sous-traitance ?

Le CEPD a adopté, le 2 septembre 2020, des lignes directrices sur les notions de responsable du traitement et de sous-traitant.

Dans ses lignes directives du 2 septembre 2020, le CEPD a fourni certains éléments d'information relatifs à la relation entre un responsable du traitement et son sous-traitant.

1. Le CEPD indique que, lorsque le responsable du traitement souhaite s'assurer que son sous-traitant présente des garanties suffisantes, au sens du RGPD, il doit évaluer :

- les connaissances du sous-traitant, notamment son expertise technique en matière de sécurité ;
- la fiabilité du sous-traitant ;
- les ressources du sous-traitant.

2. Le CEPD rappelle, au sujet du contrat de sous-traitance en tant que tel, que l'obligation de conclure celui-ci pèse à la fois sur le responsable du traitement et sur son sous-traitant.

De plus, ce contrat ne doit pas se contenter de rappeler les exigences du RGPD, il doit aussi mentionner les informations concrètes permettant de déterminer comment ces exigences seront remplies.

A ce titre, le contrat doit inclure, notamment :

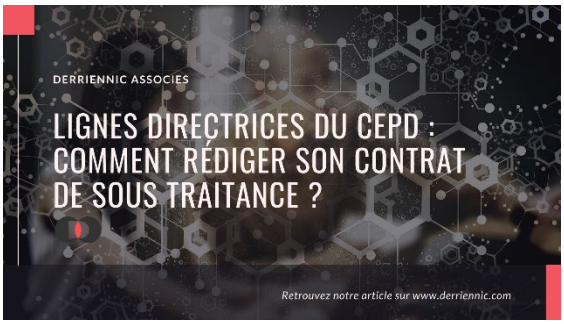
- des informations quant aux mesures de sécurités qui doivent être adoptées par le sous-traitant ;
- l'obligation du sous-traitant d'obtenir l'accord du responsable du traitement en cas de changement de ces mesures ; ainsi que
- une revue régulière desdites mesures, de sorte que les parties soient assurées de leur adéquation aux risques.

S'agissant de l'assistance due au responsable du traitement quant aux requêtes dont les personnes le saisissent afin d'exercer leurs droits, le CEPD indique que la gestion de ces requêtes peut être confiée au sous-traitant, bien que cela ne décharge pas le responsable du traitement de sa responsabilité de répondre auxdites requêtes.

S'agissant de l'obligation de notification en cas de violation de données, qui pèse sur le sous-traitant, le CEPD recommande de formaliser, dans le contrat, une durée de notification, par exemple un nombre d'heures.

Le CEPD rappelle, enfin, que le sous-traitant doit imposer à son propre sous-traitant les mêmes obligations en matière de protection de données que celles lui incombant au titre du contrat conclu avec le responsable du traitement. Cela inclut notamment l'obligation, pour le sous-traitant ultérieur, de permettre la réalisation d'audits par le responsable du traitement ou un autre auditeur qu'il aurait mandaté.

Lien vers les lignes directrices : https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf



Manquements multiples dans le traitement de données clients : 250.000 € d'amende

Le 28 juillet dernier, la CNIL a condamné la société SPARTOO à une amende de 250.000 euros pour plusieurs manquements au RGPD.

La société SPARTOO est une entreprise spécialisée dans le secteur de la vente de chaussures, qui édite seize sites web à destination de treize pays de l'Union européenne pour les besoins de son activité.

Le 31 mai 2018, soit quelques jours après l'entrée en application du RGPD, la CNIL a procédé à un contrôle sur place, dans les locaux de la société SPARTOO, afin de vérifier le respect, par cette dernière, de l'ensemble des dispositions du RGPD et de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « Loi Informatique et Libertés »). Etaient particulièrement visés les traitements de données à caractère personnel des clients et prospects, ainsi que les enregistrements des conversations téléphoniques intervenues entre les clients et le service client de la société SPARTOO.

A noter que, pour la première fois, la CNIL agissait en tant « qu'autorité chef de file », pour les traitements transfrontaliers opérés par la société SPARTOO.

Dans sa délibération du 28 juillet dernier, la CNIL a reproché à la société SPARTOO de multiples manquements au RGPD.

Tout d'abord, la CNIL a considéré que la société SPARTOO avait manqué au principe de minimisation des données, consacré à l'article 5-1 c) du RGPD. Ce manquement était constitué par :

- l'enregistrement intégral et permanent des appels téléphoniques reçus par le service client, considéré excessif au regard de la finalité du traitement (à savoir la formation des salariés) ;
- l'absence de mesures permettant d'éviter l'enregistrement des coordonnées bancaires des clients lors des appels téléphoniques, dans la mesure où la finalité du traitement était l'évaluation des salariés et que la CNIL a considéré que ces données ne pouvaient servir qu'au paiement et, ainsi, ne devaient pas être enregistrées une fois le paiement validé ; et
- une collecte de données jugée excessive dans le cadre du traitement ayant pour finalité la lutte contre la fraude : cette collecte aurait pu, selon elle, concerner uniquement la carte d'identité, mais ne se cantonnait pas à ce seul document.

Aussi, la CNIL a estimé que la société SPARTOO avait manqué à son obligation de limitation de la durée de conservation des données, prévue à l'article 5-1 e) du RGPD, du fait de :

- la mise en place d'une durée de conservation de 5 ans à compter de la dernière activité pour les données des prospects, considérée comme excessive par la CNIL, compte tenu du fait que SPARTOO s'abstenait de contacter les prospects après une période d'inactivité de 2 ans ;
- la détermination du point de départ du délai de conservation des données des prospects à l'ouverture d'un courriel de prospection, ce qui ne constitue pas un point de départ valable pour la CNIL;
- l'absence de suppression des données des clients à l'issue de la durée de conservation, les données étant seulement pseudonymisées pour permettre aux clients de se reconnecter à leur compte.

De plus, la CNIL a considéré que la société SPARTOO avait manqué à son obligation

d'information des personnes concernées consacrée à l'article 13 du RGPD puisque :

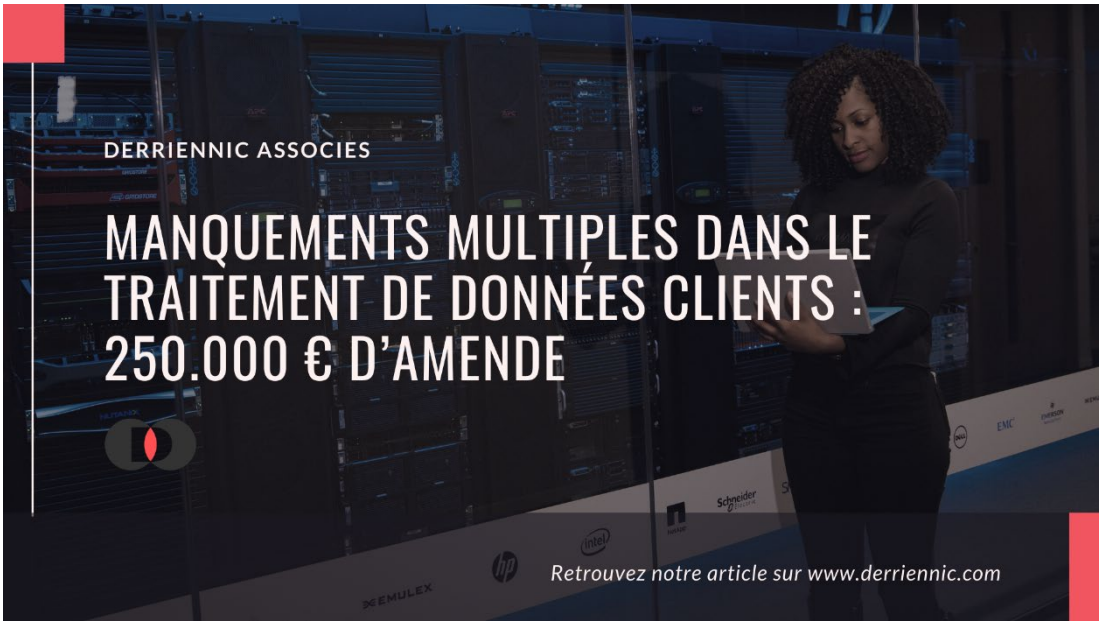
- s'agissant des clients, la société SPARTOO s'était contentée d'inscrire dans la politique de confidentialité que le consentement était la base légale de l'intégralité des traitements opérés, alors que cette base légale n'était pas la plus adaptée au regard des exigences du RGPD et qu'il convenait d'indiquer la base légale relative à chaque traitement ;
- s'agissant des salariés, la CNIL a estimé que les nouveaux salariés n'étaient ni informés de l'enregistrement de leurs conversations téléphoniques, ni de la finalité poursuivie par le traitement, de la base légale du dispositif, des destinataires des données, de la durée de conservation des données et de leurs droits à cet égard.

Enfin, la CNIL a estimé que la société SPARTOO n'avait pas respecté son obligation d'assurer la sécurité des données, prévue à l'article 32-2 du RGPD, du fait :

- de la mise en place de mots de passe insuffisamment robustes puisque composés de huit caractères, sans critère de complexité ;
- de la communication par courriel (canal non chiffré) de scans de la carte bancaire des personnes suspectées de fraude.

A la lumière de ces manquements et du nombre de personnes concernées (la CNIL a relevé plus de 3 millions d'anciens clients et plus de 25 millions de prospects concernés par une durée de conservation excessive de leurs données), la société SPARTOO a été condamnée au paiement d'une amende de 250.000 euros, complétée d'une injonction de se conformer à ses obligations au titre du RGPD dans un délai de trois mois à compter de la présente délibération, sous astreinte de 250 euros par jour de retard à l'issue de ce délai.

Lien vers la décision : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000042203965&fastReqId=655302508&fastPos=1



COVID-19 : Quelle collecte des données par l'employeur ?

Le 23 septembre dernier, la CNIL a actualisé ses recommandations concernant la collecte de données personnelles par les employeurs dans le contexte de la crise sanitaire liée au COVID-19.

Depuis le début de la crise sanitaire, et afin de lutter contre la propagation du virus, un grand nombre d'employeurs a mis en place des mesures impliquant la collecte de données de santé de ses salariés ou des visiteurs de ses locaux. Dans ce contexte, la CNIL a mis à jour ses recommandations publiées lors du déconfinement, en mai dernier.

1. Traitement de données de santé par l'employeur dans le cadre de la crise sanitaire

Pour mémoire, il résulte de la combinaison des articles 6 et 9 du RGPD que le traitement de données de santé, en tant que données sensibles, est en principe prohibé, sauf à ce que le responsable de traitement justifie qu'il bénéficie de l'une des exceptions prévues par l'article 9 du RGPD.

A ce titre, la CNIL estime que, dans le contexte du travail, les exceptions suivantes pourraient justifier la collecte par l'employeur de données de santé :

- *« la nécessité pour l'employeur de traiter ces données pour satisfaire à ses obligations en matière de droit du travail, sécurité sociale et protection sociale ;*
- *la nécessité, pour un professionnel de santé, de traiter ces données aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation (sanitaire) de la capacité de travail du travailleur, de diagnostics médicaux etc. »*

Aussi, la CNIL rappelle que l'employeur ne « *saurait prendre de mesures susceptibles de porter une atteinte disproportionnée aux libertés individuelles des salariés* » (article L.1121-1 du code du travail), telle que la collecte excessive des données de santé de ses salariés.

2. Obligations de sécurité de l'employeur et des salariés

Dans la mesure ou l'employeur est responsable de la santé et de la sécurité de ses salariés et qu'il doit ainsi, prendre toutes les mesures nécessaires à cet égard (article L4121-1 du code du travail), la CNIL estime que, dans le contexte actuel, l'employeur est notamment légitime :

- *« à rappeler à ses employés, travaillant au contact d'autres personnes, leur obligation d'effectuer des remontées individuelles d'informations en cas de contamination ou suspicion de contamination, auprès de lui ou des autorités sanitaires compétentes, aux seules fins de lui permettre d'adapter les conditions de travail ;*
- *à faciliter leur transmission par la mise en place, au besoin, de canaux dédiés et sécurisés ;*
- *à favoriser les modes de travail à distance et encourager le recours à la médecine du travail. »*

La CNIL ajoute que les salariés sont tenus de préserver leur santé et sécurité ainsi que celles des autres salariés (article L4122-1 du code du travail). De cette obligation, la CNIL déduit que les salariés, à l'exception de ceux placés en télétravail ou travaillant de manière isolée, doivent signaler à leur employeur toute contamination ou suspicion de contamination,

dès l'instant où ils ont pu exposer une partie de leurs collègues au virus.

De surcroît, la CNIL indique que si l'employeur peut légitimement traiter les données de santé dans le cadre de ces signalements, il doit veiller à ce que seules soient traitées les données strictement nécessaires pour « *prendre des mesures organisationnelles de formation et d'information, ainsi que certaines actions de prévention des risques professionnels* ».

Enfin, la CNIL précise que l'employeur ne doit, à aucun moment, communiquer aux autres employés l'identité du salarié susceptible d'être infecté.

3. Précisions sur la position de la CNIL sur certaines pratiques

Dans le prolongement de ses recommandations publiées aux mois de mars et mai derniers, la CNIL a apporté des précisions sur des pratiques mises en œuvre par de nombreux employeurs dans le contexte de la crise sanitaire.

- **S'agissant des relevés de température**

La CNIL estime « *qu'en l'état du droit, et sauf à ce qu'un texte en prévoit expressément la possibilité, il est interdit aux employeurs de constituer des fichiers conservant des données de températures de leurs salariés* ». De même, la CNIL ajoute qu'est également interdite la mise en place d'outils de captation automatique de température, telles que des caméras thermiques.

Enfin, la CNIL rappelle que les contrôles de températures « *manuels* » mis en œuvre sans qu'aucune donnée ne soit conservée, ne relèvent pas de la règlementation en matière de protection des données personnelles mais du droit social. La CNIL renvoie donc aux recommandations du Ministère du travail à cet égard, lequel recommande de ne pas mettre en œuvre de contrôle de la température à des fins de dépistage du COVID-19.

- **S'agissant des tests sérologiques et de questionnaires sur l'état de santé**

Selon la CNIL, les données relatives à l'état de santé de la personne concernée, y compris le résultat d'un éventuel test de dépistage du COVID-19, ainsi que des données relevant de leur sphère privée ne peuvent être collectées et traitées que par les professionnels de santé soumis au secret médical.

Aussi, la CNIL rappelle que le Ministère du travail n'autorise pas « *les campagnes de dépistage organisées par les entreprises pour leurs salariés* ».

- **S'agissant des plans de continuité de l'activité (« PCA »)**

Dans le contexte actuel de crise sanitaire, la CNIL souligne que l'employeur peut mettre en œuvre un PCA pour maintenir l'activité essentielle et, à ce titre, *« créer un fichier nominatif pour l'élaboration et la tenue du plan qui ne doit contenir que les données nécessaires à la réalisation de cet objectif* ».

- **S'agissant de la réorganisation du travail**

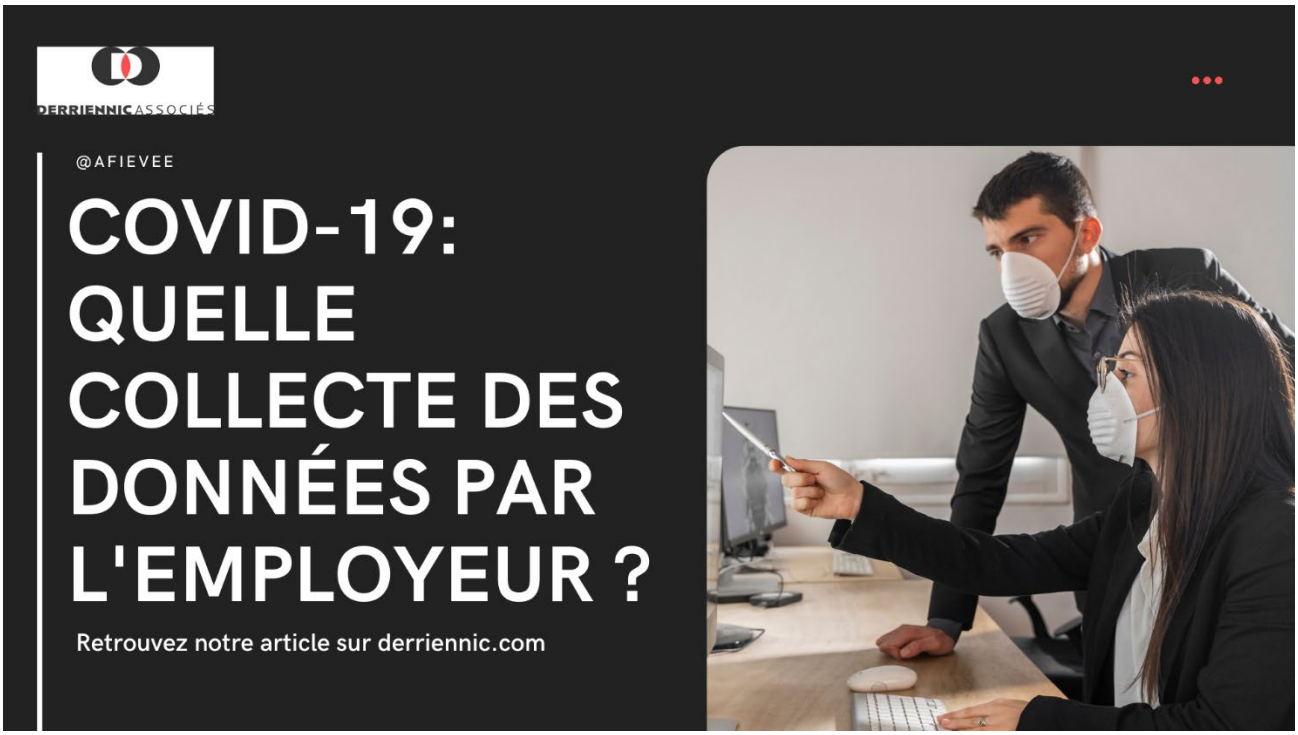
Dans le cadre du déploiement de mesures afin de protéger la santé des salariés face au risque de propagation du COVID-19, la CNIL rappelle tout d'abord qu'il résulte de son obligation de sécurité que l'employeur doit prendre des mesures de protection collective de prévention, telles que le rappel des gestes barrières et de la distanciation sociale ou encore la fourniture de solution hydroalcoolique.

Selon la CNIL, l'employeur ne doit pas organiser la collecte de données de santé de l'ensemble des salariés. L'employeur doit se contenter de prendre des mesures individuelles, comme par exemple le télétravail, à la suite d'un signalement par le salarié de sa suspicion de contamination, durant une courte période, le temps que le salarié concerné consulte un professionnel.

A ce titre, la CNIL précise que seul le service de santé au travail peut collecter des données de santé, notamment relative à la vulnérabilité ou du risque d'exposition du salarié au COVID-19. Il peut ainsi proposer des conditions individualisées de travail telles que l'aménagement ou l'adaptation du poste ou du temps de travail du salarié. Selon la CNIL, l'employeur doit se contenter d'appliquer les mesures proposées.

Liens des communiqués cités :

https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles-par-les#donn%C3%A9es-sant%C3%A9



L'autorité de protection des données d'Hambourg prononce une sanction pécuniaire record de 35,3 millions d'euros

L'autorité de protection des données d'Hambourg a prononcé une importante sanction à l'encontre d'une société H&M localisée à Nuremberg pour atteinte grave à la vie privée de ses employés.

L'affaire concerne un cas de surveillance de plusieurs centaines d'employés d'une société H&M localisée à Nuremberg.

Dans son communiqué de presse, le régulateur expose que, depuis 2014, une partie des employés faisait l'objet d'enregistrements concernant de nombreux détails relatif à leur vie privée :

- Les « notes de correspondance » étaient stockées en permanence sur le réseau ;
- Après une absence (vacance ou arrêt maladie, même de courte durée), le management réalisait des « Welcome back talks » (discussion de retour) avec leurs employés, dont le contenu était enregistré ;
- De plus, certains managers disposaient d'une grande connaissance de la vie privée de leurs employés grâce aux discussions informelles, allant du plus petit détail aux questions familiales ou de croyances religieuses.

Ces informations, enregistrées et stockées numériquement, étaient rendues accessibles à une cinquantaine de managers au sein de l'entreprise. Celles-ci étaient non seulement utilisées dans le cadre d'une évaluation méticuleuse des performances individuelles au travail, mais également, pour établir un profil détaillé des employés.

Ces pratiques ont été révélées au grand jour à la suite d'un problème technique, ayant rendu accessible ces données dans l'entreprise.

C'est après avoir été informée de ce traitement dans la presse, que l'autorité d'Hambourg a ordonné, d'une part, une limitation du traitement (que ces contenus stockés sur le serveur soient « gelés ») et, d'autre part, une remise des données pour analyse.

À la suite de cet incident, les responsables ont pris diverses mesures correctives. L'autorité relève que la direction de l'entreprise a présenté des excuses expresses aux personnes concernées, et également suivi la suggestion de verser aux employés un « dédommagement considérable ». C'est, pour elle, une reconnaissance sans précédent par une société de sa responsabilité à la suite d'un tel incident relatif à la protection des données.

Un commissaire de l'autorité de protection des données d'Hambourg a commenté en indiquant qu'il s'agissait d'un grave manquement à la protection des données des employés et que le montant de l'amende était adéquat et effectif pour dissuader les sociétés de violer la vie privée de leurs employés.