# NEWSLETTER RGPD/DATA

NUMÉRO 48 ● NOVEMBRE 2022

SOMMAIRE



**FORMATION A LA PREPARATION A LA CERTIFICATION « DPO ».**
**DATE SUR DEMANDE**

# REGLEMENT DSA : LA PROCEDURE D'ADOPTION TOUCHE A SA FIN

*Ce mois-ci, le DSA a été approuvé définitivement par le Conseil de l'UE puis signé par ce dernier et le Parlement européen, marquant ainsi la fin d'un long processus d'adoption et le début d'une nécessaire mise en conformité pour de nombreuses plateformes.*

Pour mémoire, le DSA pour « Digital Service Act » est un règlement européen, dont le nom officiel est « *règlement relatif à un marché unique des services numériques et modifiant la Directive 2000/31/CE (Règlement sur les services numériques)* », proposé par la Commission européenne le 15 décembre 2020.

Ce règlement encadre principalement le fonctionnement des « intermédiaires en ligne » afin de réguler davantage les contenus illicites en ligne et ce, en adaptant l'actuelle Directive dite « E-commerce » (directive n°2000/31/CE sur le commerce électronique, transposée dans notre « LCEN »), aux évolutions du marché numérique. Ce texte met à jour les obligations et responsabilités des plateformes d'e-commerce mais aussi et, plus largement, définit les obligations et responsabilités des fournisseurs de services intermédiaires en ligne tels que les réseaux sociaux, les places de marchés en ligne, les plateformes de partage de contenus, les services cloud et les FAI. Des obligations supplémentaires sont également prévues pour les « *très grandes plateformes en ligne* » et les « *très grands moteurs de recherche* », c'est-à-dire ceux comptant plus de 45 millions d'utilisateurs actifs chaque mois au sein de l'UE.

Le Conseil de l'UE et le Parlement européen avait trouvé un accord provisoire sur le texte le 23 avril dernier. Le 4 octobre 2022, le Conseil de l'UE a approuvé définitivement le texte. Aussi, le 19 octobre 2022, le texte final a été signé par le Conseil de l'UE et le Parlement européen. Sa publication au Journal Officiel de l'UE ne devrait plus tarder.

Le règlement DSA sera applicable dans un délai de 15 mois à compter du 20ème jour suivant cette publication, sauf pour les « *très grandes plateformes* » et les « *très grands moteurs de recherche* » qui disposeront d'un délai réduit de 4 mois à compter de la notification de leur désignation conformément au DSA.

Les acteurs concernés sont donc invités à commencer, dès à présent, leur démarche de mise en conformité, dont l'ampleur peut être importante (revue des processus de traitement des réclamations/litiges et des documents contractuels dont les CGV, etc.), étant rappelé qu'une non-conformité peut être passible d'une amende pouvant aller jusqu'à 6% de leur chiffre d'affaires mondial total.

**Source** : ici

# VIOLATION DE DONNEES : DES NOUVELLES LIGNES DIRECTRICES DU CEPD ?

*Le 18 octobre dernier, le CEPD a publié et soumis à consultation publique des nouvelles lignes directrices sur la notification des violations de données à caractère personnel. En réalité, il s'agit d'une simple mise à jour des exigences concernant la notification d'une violation de données par un organisme non établi dans l'UE.*

Pour mémoire, des lignes directrices sur la notification des violations des données à caractère personnel, référencées « *WP250 (rev.01)* », avaient été approuvées par le CEDP le 25 mai 2018.

Le 18 octobre dernier, le CEPD a publié des nouvelles lignes directrices référencées « *Lignes directrices 09/2022 sur la notification de violation de données en application du RGPD* ».

Ces lignes directrices consistent, en réalité, en une « *légère mise à jour* » des lignes directrices « *WP250 (rev.01)* ».

En sus de modifications purement rédactionnelles, la mise à jour apporte une, et une seule, modification de fond concernant les exigences de notification pour les organismes situés hors UE.

Pour rappel, des organismes non établis dans l'UE sont soumis aux obligations de notification en cas de violation concernant un traitement de données à caractère personnel de personnes situées dans l'UE (traitement entier avec une offre de biens ou de services ou le suivi de leur comportement au sein de l'UE).

La nouvelle version proposée par le CEPD (09/2022), propose un mécanisme radicalement différent : « *la simple présence d'un représentant dans un État membre ne déclenche pas le système du guichet unique. C'est pourquoi la violation devra être notifiée à l'autorité de contrôle de chaque Etat membre dans lequel les personnes concernées résident* ».

En d'autres termes, la proposition revient à exiger d'un organisme établi hors UE de notifier une violation de données personnelles (i) non pas auprès de l'autorité de contrôle de l'Etat membre dans lequel son représentant de l'UE désigné est établi ; (ii) mais auprès de l'autorité de contrôle de l'Etat membre dans lequel réside les personnes concernées par la violation, c'est à dire potentiellement auprès de plusieurs autorités de contrôle, évitant ainsi le « forum shopping » mais complexifiant d'autant les démarches à réaliser.

A suivre…

**Source** : ici

# TRAITEMENT DE DONNEES PERSONNELLES DE MINEURS : UNE AMENDE HISTORIQUE POUR INSTAGRAM

*Le 15 septembre 2022, l'autorité de contrôle irlandaise (Data Protection Commission) a sanctionné Instagram pour avoir traité les données personnelles de mineurs en contradiction avec le RGPD.*

En 2020, l'autorité de contrôle irlandaise a, de sa propre initiative, ouvert une enquête à l'encontre d'Instagram.

Cette enquête a révélé plusieurs carences du réseau social. L'autorité de contrôle irlandaise a reproché à Instagram (i) de paramétrer par défaut les comptes personnels de mineurs comme « public », permettant à n'importe quel utilisateur de la plateforme d'accéder aux informations du profil et aux photos et (ii) de communiquer par défaut les coordonnées (courriel et numéro de téléphone) de mineurs ayant un compte professionnel.

Ces carences constituent, selon l'autorité de contrôle, des manquements au RGPD, et notamment à :

- l'article 12, dès lors que le mineur n'a pas été informé de manière claire et transparente sur la publication de ses coordonnées et le paramétrage par défaut en mode « public » ;
- l'article 35§1, dès lors qu'Instagram n'a pas réalisé d'analyse d'impact pour ces deux traitements ;
- l'article 5§1, dès lors qu'Instagram n'a pas respecté le principe de minimisation du traitement des données ;
- l'article 25§1, dès lors qu'Instagram n'a pas mis en œuvre les mesures techniques et organisationnelles appropriées, (telles que la pseudonymisation), pour protéger les données des mineurs.

Le projet de décision de l'autorité de contrôle irlandaise a fait l'objet d'objections de la part d'autres autorités de contrôle nationales.

A défaut de consensus entre les autorités de contrôle, et conformément au processus de règlement des différends prévus à l'article 65 du RGPD, le Comité européen pour la protection des données (CEPD) a pris, le 28 juillet 2022, une décision contraignante.

Le CEPD a ainsi enjoint à l'autorité irlandaise de :

- modifier son projet de décision pour ajouter une violation de l'article 6 du RGPD. Effectivement, Instagram indiquait comme base légale de ses traitements l'exécution du contrat avec l'utilisateur ou l'intérêt légitime de l'entreprise. Or, le CEPD a jugé que les traitements effectués par Instagram ne reposaient sur aucune base légale dès lors (i) que la publication des coordonnées du mineur n'était pas nécessaire à l'exécution du contrat et, (ii) que l'intérêt légitime d'Instagram ne prévalait pas sur les libertés et droits fondamentaux des mineurs utilisant la plateforme.

- réévaluer l'amende à la hausse, afin que cette dernière soit effective, proportionnée et dissuasive, conformément à l'article 83 du RGPD.

Compte tenu de ce qui précède, l'autorité de contrôle irlandaise a pris en compte ces injonctions et a prononcé une amende de 405 millions d'euros à l'encontre d'Instagram.

**Source** : ici

# TRAITEMENT DE DONNEES POUR UNE FINALITE « COMPATIBLE » : LES PRECISIONS DE LA CJUE

*La CJUE s'est récemment prononcée sur la notion de finalité « compatible » d'un traitement de données réalisé sans le consentement des personnes concernées et ce, afin d'apprécier la légalité d'un tel traitement.*

En raison d'une défaillance technique affectant le fonctionnement d'un de ses serveurs, une société fournissant des services internet et de télévision, la société Digi, a créé une base de données « tests », dans laquelle elle a copié des données personnelles de certains de ses clients.

Ces données copiées étaient conservées, par ailleurs, dans une autre base de données, plus opérationnelle contenant (i) les données des personnes s'étant inscrites à la lettre d'actualité de la société Digi et (ii) des données d'administrateur système donnant accès à l'interface de son site.

La société Digi a fait l'objet d'une sanction (200.000 € d'amende) prononcée par l'autorité de protection des données hongroise pour violation du principe de « limitation des finalités » (principe selon lequel les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités) et du principe de « limitation de la conservation des données » (principe selon lequel les données personnelles doivent être conservées sous une forme permettant d'identifier les personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées), deux principes consacrés par l'article 5 du RGPD.

En effet, la société Digi a supprimé la base « tests » seulement 18 mois après avoir corrigé la défaillance technique.

Contestant la position de la « CNIL » hongroise, la société Digi a formé un recours devant la juridiction locale laquelle s'est tournée vers la CJUE en interprétation notamment du principe de la « limitation des finalités » au sens du RGPD.

Dans son arrêt du 20 octobre dernier, la CJUE a jugé que la « limitation des finalités » ne s'oppose pas, par principe, à l'enregistrement et la conservation par le responsable de traitement dans une base de données créée aux fins de procéder à des tests et de corriger des erreurs, de données personnelles préalablement collectées et conservées dans une autre base de données.

Toutefois, la CJUE a souligné qu'un tel traitement doit être compatible avec les finalités spécifiques pour lesquelles les données personnelles ont été initialement collectées et ce, conformément à l'article 6.4 du RGPD (relatif aux conditions de licéité d'un traitement (i) à une fin autre que celle pour laquelle les données ont été collectés et (ii) intervenant sans le consentement de la personne concernée).

Si cette appréciation revient à la juridiction nationale, la CJUE a apporté des clés d'appréciation. La CJUE a ainsi relevé que la réalisation de tests et la correction d'erreurs affectant la base de données client présente un lien concret avec l'exécution des contrats d'abonnements de la société Digi.

En effet, ces erreurs sont susceptibles d'être dommageables pour la fourniture du service contractuellement prévu et pour laquelle les données ont été initialement collectées. Pour les juges européens, ce traitement ne s'écarte ainsi pas des attentes légitimes des clients quant à l'utilisation ultérieure de leurs données. En outre, la CJUE a relevé que la « CNIL » hongroise n'a pas fait état de données sensibles figurant dans cette base, ni de conséquences dommageables de ce traitement ultérieur pour les clients, pas plus que d'une absence de garanties appropriées prises par la société Digi.

En revanche et sans surprise, la CJUE a jugé que le principe de la « limitation de la conservation » s'oppose à la conservation par le responsable de traitement, dans une base de données créée aux fins de procéder à des tests et de corriger des erreurs, des données personnelles préalablement collectées pour d'autres finalités, pour une durée excédant celle qui est nécessaire à la réalisation de ces tests et à la correction de ces erreurs.

Cette décision illustre l'approche concrète que doivent suivre les juges pour apprécier une finalité « compatible » au sens du RGPD, approche particulièrement précieuse pour l'analyse de la légalité de traitements de données « ultérieur ».

**Source :** ici

# DEFAUT DE BASE LEGALE : CLEARVIEW CONDAMNEE A 20 MILLIONS D'EUROS D'AMENDE

*Le 17 octobre 2022, la CNIL a prononcé à l'encontre de la société américaine Clearview une amende administrative de 20 millions d'euros, pour défaut de base légale et non prise en compte satisfaisante des demandes d'exercice des droits des personnes concernées.*

Clearview, société établie aux Etats-Unis, a développé un logiciel de reconnaissance faciale, dont la base de données repose sur l'« *aspirage d'images publiquement accessibles sur internet* », et qui permet d'identifier une personne à partir d'une photographie la représentant.

Entre mai et décembre 2020, la CNIL a reçu des réclamations émanant de personnes concernées par ce traitement, qui rencontraient des difficultés dans le cadre de l'exercice de leurs droits d'accès et d'effacement auprès de Clearview.

La CNIL a procédé à un contrôle sur pièces portant sur les traitements mis en œuvre par Clearview et a sollicité la communication d'informations de la part des autres autorités de contrôle concernées. Il en est ressorti que Clearview collecte des photographies sur les réseaux sociaux, à partir desquelles elle calcule un gabarit biométrique. Clearview commercialise l'accès à un moteur de recherche en ligne permettant de calculer une « *empreinte numérique* » à partir d'une photographie communiquée par un client, généralement les forces de l'ordre. Clearview recherche les photographies présentes dans sa base de données ayant une empreinte similaire, ce qui, *In fine*, permet d'identifier la personne de façon unique à partir d'une photographie la représentant.

La seconde question était la suivante : est-ce que la publication sur le site internet de l'autorité publique concernée de données à caractère personnel susceptibles de divulguer indirectement les opinions politiques, l'appartenance syndicale ou l'orientation sexuelle d'une personne physique constitue un traitement de données sensibles au sens du RGPD ?

La CJUE a relevé que si les données concernées ne constituent pas par leur nature des données sensibles au sens de ces textes, elles sont de nature à révéler, par une opération intellectuelle de rapprochement ou de déduction, l'orientation sexuelle d'une personne physique et, de ce fait, rentrent dans la catégorie de données sensibles.

Cette position des juges européens apporte des clarifications à la qualification de données sensibles : sont concernées, au-delà des données sensibles par nature, les données révélant des données sensibles par simple rapprochement ou déduction intellectuels.

Une telle décision invite ainsi les responsables de traitement et sous-traitants à la plus grande vigilance dans leurs traitements de données, les cas de qualification de données sensibles étant particulièrement larges. A suivre la CJUE, de simples données de géolocalisation ou de consommation et d'habitude alimentaires pourraient effectivement permettre de déduire la religion d'une personne et pourraient être qualifiées de données sensibles.

**Source :** ici

# LE CONSEIL D'ETAT DRESSE LES LIMITES DE LA PROTECTION DU DPO

*Dans une décision du 21 octobre 2022, le Conseil d'Etat a statué sur une décision de la CNIL ayant rejeté la demande d'un DPO concernant l'exercice de son droit d'accès et de ses fonctions en qualité de DPO.*

Une personne exerçant des fonctions de délégué à la protection des données (« DPO ») a saisi la CNIL d'une plainte contre sa propre société, au motif (i) que l'exercice de son droit d'accès n'aurait pas connu les suites espérées et (ii) que les conditions d'exercice de ses fonctions de DPO ne seraient pas satisfaisantes. Le DPO reprochait notamment à son employeur (i) de lui avoir donné des instructions, (ii) de ne pas lui avoir octroyé le taux maximum d'une de ses primes de performance et (iii) de l'avoir licencié.

La plainte avait été rejetée par la CNIL, à la fois s'agissant de l'exercice du droit d'accès et s'agissant de l'exercice des fonctions de DPO. Sur ce dernier point, la CNIL avait considéré que l'exigence de protection de l'indépendance fonctionnelle du DPO ne faisait pas obstacle à ce que la société « *puisse reprocher à l'intéressée des carences dans l'exercice de ses fonctions ainsi que le non-respect des règles internes à la société, dont il n'était pas allégué qu'elles étaient incompatibles avec l'indépendance fonctionnelle du délégué* ».

Le DPO a formé un recours devant le Conseil d'Etat afin d'obtenir l'annulation de la décision de rejet émanant de la CNIL l'estimant insuffisamment motivée. Le Conseil d'Etat, dans une décision du 21 octobre 2022, a rejeté la requête du DPO, en statuant comme suit.

**1. Droit d'accès : une motivation nécessaire et, en l'espèce, suffisante, du rejet**

S'agissant de l'exercice du droit d'accès de la requérante, le Conseil d'Etat a indiqué que la décision de rejet de la CNIL « *comporte l'énoncé des considérations de droit et de fait qui en constituent le fondement* » et, qu'en conséquence, « *la requérante n'est (…) pas fondée à soutenir que cette décision serait entachée d'insuffisance de motivation* ».

**2. Exercice des fonctions de DPO : la CNIL n'a pas à motiver son rejet**

S'agissant de l'exercice estimé insatisfaisant de ses fonctions de DPO par la requérante, le Conseil d'Etat a considéré que le rejet de la CNIL « *n'est pas au nombre des décisions individuelles défavorables énumérées à l'article L. 211-2 du code des relations entre le public et l'administration* ».

En particulier, cette décision « *ne constitue ni une mesure restreignant l'exercice des libertés publiques, ni le refus d'un avantage dont l'attribution constitue un droit pour les personnes qui remplissent les conditions légales pour l'obtenir, eu égard au large pouvoir d'appréciation dont bénéficie la CNIL, saisie d'une plainte qui n'est pas fondée sur l'un des droits individuels reconnus par le RGPD à la personne concernée* ».

Ainsi, la juridiction administrative a considéré qu'aucun texte n'imposait à la CNIL de motiver sa décision.

**3. Les précisions du Conseil d'Etat quant à la protection des DPO**

Le DPO bénéficie d'un régime de protection garanti par l'article 38.3 du RGPD, qui indique que le DPO ne peut pas « *être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions* ».

La CNIL a eu l'occasion de préciser, dans son guide pratique sur le DPO, que cela signifie que le DPO ne peut pas être inquiété pour des analyses ou remarques fondées en matière de protection des données qu'il adresserait aux opérations de traitement de son employeur, et que « *le licenciement abusif d'un DPO constituerait une infraction au RGPD* ». En revanche, pour la CNIL, le DPO peut être licencié pour des motifs autres que l'exercice de ses missions de délégué : vol, harcèlement moral, autres fautes graves similaires, etc.

Dans sa décision du 21 octobre 2021, le Conseil d'Etat a apporté des éclairages supplémentaires sur la relation entre le DPO et son employeur.

Il y est indiqué que la protection du DPO au titre du RGPD vise « *essentiellement à préserver l'indépendance fonctionnelle* » du DPO et, partant, à « *garantir l'effectivité des dispositions du RGPD* ». Cette protection ne fait pas, en revanche, obstacle au licenciement d'un DPO qui ne posséderait plus les compétences nécessaires à l'exercice de ses fonctions, ou « *qui ne s'acquitterait pas de celles-ci conformément aux dispositions du RGPD* ».


**Source : ici**

DOCTRINE

RGPD

# BtoC : enregistrements audio des conversations des clients

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question soumise à l'autorité hongroise de protection des données relative à la licéité des enregistrements audio réalisés par une entreprise à des fins probatoires et notamment pour se prémunir contre d'éventuelles réclamations de clients.

Selon la Cnil, l'enregistrement de conversations téléphoniques à des fins de preuve de la formation d'un contrat est licite, à condition d'être nécessaire.

Ainsi, un organisme souhaitant enregistrer des conversations téléphoniques à des fins probatoires doit démontrer qu'il ne dispose pas d'autres moyens pour prouver qu'un contrat a été conclu avec la personne concernée. Par ailleurs, la Cnil ajoute que le principe de minimisation doit être respecté : « *Sauf dispositions légales le permettant, les enregistrements ne peuvent être ni permanents ni systématiques. Seules les conversations portant sur la conclusion d'un contrat par voie téléphonique peuvent être enregistrées. Le professionnel devra ainsi prévoir des mécanismes afin de n'enregistrer la conversation téléphonique entre le téléopérateur et le consommateur qu'à partir du moment où son objet porte clairement sur la conclusion d'un contrat. La partie pertinente de la conversation ne peut être conservée qu'en l'absence d'une autre modalité de preuve de la formation du contrat ou de son exécution, telle qu'une confirmation écrite.* »[1]

Bien entendu, les personnes concernées par l'enregistrement (clients et personnel de l'entreprise) doivent être informées de façon concise, transparente, compréhensible et selon un mode aisément accessible, en des termes clairs et simples, de la manière dont le traitement est réalisé.

Dans le cas d'espèce, les enregistrements ne portaient pas sur des conversations téléphoniques mais sur des échanges oraux en face-à-face entre les clients et les salariés de l'entreprise intervenant au domicile desdits clients.

## L'affaire[2]

Une plainte a été déposée contre une entreprise de rénovation, au motif que ses employés effectuaient, avec leurs téléphones mobiles, des enregistrements audio des conversations, lors de leurs interventions sur site. Devant l'autorité de contrôle, l'entreprise a justifié cette pratique par la nécessité de documenter les échanges qui intervenaient pendant les travaux car, dans de nombreux cas, les clients – pour la plupart des personnes âgées – contestaient après coup avoir correctement été informés sur les conditions du chantier et notamment sur le coût de l'installation, le prix des matériaux ou encore la durée des travaux. L'autorité hongroise de protection des données a considéré qu'un tel traitement de données personnelles (l'enregistrement des conversations) était illicite.

Après avoir rappelé qu'en application de l'article 5.1 b) du RGPD les données ne peuvent être collectées que pour des finalités « *déterminées, explicites et légitimes* », l'autorité de contrôle a estimé que de tels enregistrements sonores pouvaient se justifier eu égard aux objectifs annoncés par l'entreprise de rénovation. Toutefois, elle a aussi considéré que le responsable du traitement aurait très bien pu parvenir au même résultat en faisant remplir et signer à ses clients une feuille de travail certifiant le contenu des échanges intervenus pendant la durée des opérations. En d'autres termes, un tel traitement n'était pas légitime en l'espèce puisqu'il existait d'autres moyens pour atteindre l'objectif probatoire, et ce sans avoir besoin de recourir aux enregistrements sonores. Par ailleurs, l'autorité de contrôle a jugé cette pratique disproportionnée non seulement en termes de durée d'enregistrement (puisque

potentiellement cette durée pouvait correspondre à celle des travaux), mais aussi en termes de contenu (dès lors qu'on ne pouvait savoir à l'avance ce qui serait enregistré, avec le risque que des informations totalement indépendantes de la finalité du traitement puissent être collectées).

L'autorité de contrôle hongroise a également relevé que la base légale du traitement faisait défaut. Car si l'intérêt légitime pouvait être invoqué par le responsable du traitement, encore fallait-il qu'il démontre que les enregistrements audio étaient nécessaires à la réalisation de cet intérêt légitime et que cet intérêt n'était pas contre-balancé par celui des personnes concernées, en l'occurrence celui de ses clients. Faute d'avoir mis en « *balance les intérêts* » des uns et des autres, l'entreprise de rénovation a violé les dispositions de l'article 6 du RGPD.

Enfin, les mentions d'information obligatoires de l'article 13 du RGPD faisaient défaut, malgré les déclarations du responsable du traitement qui soutenait qu'au moment des enregistrements, l'information était donnée oralement. Mais faute de rapporter la preuve d'une telle information orale, l'autorité de contrôle a estimé que le responsable du traitement avait manqué à ses obligations de transparence, et ce d'autant que la feuille de travail qu'il remettait à ses clients se contentait d'avertir ces derniers que des enregistrements audio pouvaient être réalisés mais sans faire référence aux mentions obligatoires de l'article 13 du RGPD (la finalité du traitement, la base légale, les destinataires, la durée de conservation des données, les droits des personnes, etc.).

## Quelles recommandations ?

On l'aura compris, si l'enregistrement audio à des fins probatoires des conversations semblejuridiquement possible, il appartient à l'organisme, en tant que responsable du traitement, de démontrer qu'il ne dispose pas d'autres moyens pour prouver qu'un contrat a été conclu avec la personne concernée ou qu'un accord (oral) a été trouvé par les parties visant à amender un contrat déjà conclu par ailleurs.

En application du principe d'« *accountability* », cette démonstration devra être scrupuleusement documentée, au même titre d'ailleurs que la « *balance des intérêts* » s'il fonde son traitement sur l'intérêt légitime. A noter que, s'agissant des enregistrements téléphoniques, la Cnil considère que le traitement peut avoir pour base légale non pas l'intérêt légitime, mais l'exécution du contrat[3]. Enfin, il est fondamental que le responsable du traitement circonscrive le contenu de l'enregistrement à ce qui est strictement nécessaire au regard de la finalité pour laquelle un tel traitement est réalisé.

**Alexandre FIEVEE**
*Avocat Associé*
*Alice Robert*
*Avocat senior*

*Derriennic Associés*

**Notes**

(1) https://www.cnil.fr/fr/lenregistrement-des-conversations-telephoniques-afin-detablir-la-preuve-de-la-formation-dun-contrat

(2) Autorité hongroise de protection des données, numéro de l'affaire : NAIH-2801-17/2022.

(3) https://www.cnil.fr/fr/lenregistrement-des-conversations-telephoniques-afin-detablir-la-preuve-de-la-formation-dun-contrat.

## PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

### Le profilage d'une personne pour en déduire son état de santé est sanctionnable

ICO (Angleterre), 5 octobre 2022

*L'autorité de contrôle anglaise a prononcé une amende à l'encontre de EasyLife pour avoir profilé des individus sans leur consentement afin d'en déduire leur état de santé.*

A la suite de nombreuses plaintes relatives à des démarchages téléphoniques non sollicités, l'autorité de contrôle anglaise a ouvert une enquête à l'encontre de la société EasyLife.

Au cours de son enquête, l'autorité de contrôle a constaté qu'entre le 1er août 2019 et le 19 août 2020 la société avait effectué 1 345 732 appels marketing non sollicités.

Plus encore, l'autorité de contrôle a remarqué que la société ciblait des personnes ayant acheté des produits à vertu thérapeutique afin de déduire leur état de santé puis de les démarcher en leur proposant d'autres produits liés à la santé.

Après avoir rappelé que les informations sur les achats sont des données personnelles, l'autorité de contrôle a considéré que le fait d'utiliser de telles informations pour sélectionner des clients et les démarcher téléphoniquement était constitutif d'un profilage et que ledit profilage, effectué sur l'état de santé, était constitutif d'un traitement de données sensibles.

Compte tenu de ce qui précède, l'autorité de contrôle a conclu qu'EasyLife a enfreint, d'une part, l'article 13 du RGPD en ce que les personnes n'étaient pas informées de l'existence d'un profilage, d'autre part, les articles 6 et 9 du RGPD, dès lors que les personnes concernées ne consentaient pas explicitement à ce que leurs données de santé soient traitées (et plus généralement que le responsable du traitement ne disposait d'aucune base légale), et enfin, l'article 5 du RGPD, dès lors que le traitement « *invisible* » de ces données sensibles était constitutif d'un traitement déloyal, illicite et non conforme au principe de transparence du RGPD.

En conséquence, l'autorité de contrôle a infligé à EasyLife une amende de 1 350 000 livres.

**Source :** ici

# L'interdiction, pour un recruteur, de se renseigner sur la situation financière d'un candidat sans son consentement

AEPD (Espagne), 24 mai 2022

*L'autorité de contrôle espagnole a sanctionné un recruteur qui s'est renseigné sur la situation financière d'un candidat sans son consentement.*

Souhaitant embaucher un juriste, un recruteur a déposé une offre d'emploi sur une plateforme de recrutement.

Avant de prendre contact avec le candidat ayant postulé, le recruteur a effectué des investigations complémentaires et a notamment consulté le registre de l'ASNEF (Association nationale des établissements de crédit financier) afin d'obtenir des informations sur la solvabilité et la notation financière (credit rating) du candidat.

Quelques semaines plus tard, le candidat a reçu de l'ASNEF un historique des requêtes le concernant, révélant la recherche effectuée par le recruteur. Il a immédiatement porté plainte devant l'autorité de contrôle espagnole.

Dans le cadre de l'enquête menée par cette dernière, le recruteur s'est défendu en indiquant que : (i) le candidat n'avait pas été recruté, et donc que les données avaient été détruites (ii) ; la consultation de telles informations est « *habituelle* » pour les postes à responsabilité ou pour recruter des entrepreneurs individuels et professions libérales (comme des avocats) et donc que la consultation de ces informations a été effectuée par erreur pour ce juriste ; et, enfin, (iii) des mesures avaient été prises pour éviter que des incidents similaires ne se reproduisent.

Compte tenu de ce qui précède, l'autorité de contrôle a infligé au recruteur une amende d'un montant de 42 000 euros.

**Source** : ici

# Un fournisseur d'énergie sanctionné pour avoir transféré les données personnelles d'un client

AEPD (Espagne), 23 août 2022

*L'autorité de contrôle espagnole a sanctionné un fournisseur d'énergie pour avoir transféré à un inconnu les factures d'une cliente sans le consentement de cette dernière.*

Une cliente, constatant que son adresse mail avait été modifiée et que ses dernières factures avaient été transférées à un inconnu par son fournisseur de gaz et d'électricité (le « *Fournisseur* »), a déposé une plainte auprès de l'autorité de contrôle espagnole.

L'enquête menée par l'autorité de contrôle a révélé que l'inconnu s'était présenté comme un parent de la cliente et avait contacté le service client du Fournisseur afin d'obtenir un duplicata des dernières factures d'électricité.

Face à une telle demande, le Fournisseur avait mis en œuvre sa « *politique de sécurité* » et exigé de l'inconnu certaines informations qui ne sont, en principe, connues « *que par le titulaire du contrat, ou par une personne autorisée par le titulaire* ». Ainsi, l'inconnu a dû fournir (i) le nom et le prénom de la cliente, (ii) son numéro d'identification (iii) son adresse et (iv) la référence du contrat. Plus encore, l'inconnu a transmis au Fournisseur la carte d'identité de la cliente et les 4 derniers chiffres du compte bancaire.

L'autorité de contrôle, rappelant le contenu des articles 5 et 32 du RGPD, a considéré que le responsable du traitement doit, en plus d'assurer la sécurité du traitement, avoir une démarche « *proactive* » et doit pouvoir démontrer le respect du RGPD.

Or, en l'espèce, l'autorité de contrôle a considéré que le Fournisseur a violé (i) les principes d'intégrité et de confidentialité des données car, malgré les mesures de sécurité mises en œuvre, le Fournisseur a permis, à un tiers, d'accéder aux données à caractère personnel d'un client sans son consentement, et (ii) l'obligation de sécurité des traitements dès lors que les mesures de sécurité mises en place n'ont pas été suffisantes pour prévenir la violation de données personnelles.

En conséquence, le Fournisseur s'est vu infligé une amende de 48 000 euros.

**Source :** ici

# ACTUALITÉS DU CABINET

## DERRIENNIC ASSOCIÉS PROPOSE UN PROGRAMME DE FORMATION DE 35 HEURES POUR LA PRÉPARATION À LA CERTIFICATION DPO

## OBJECTIFS

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
01.47.03.14.94
afievee@derriennic.com

**CLASSEMENTS**

Alexandre Fievee figure dans le classement BestLawyers dans la catégorie « *Information Technology Law* » (2023).
Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie « *Next Generation Partners* ».

### RENSEIGNEMENTS PRATIQUES

**Prochaine session en 2022/2023 :**
Sur demande.
**Lieu de la formation :**
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.
**Inscription et informations :**