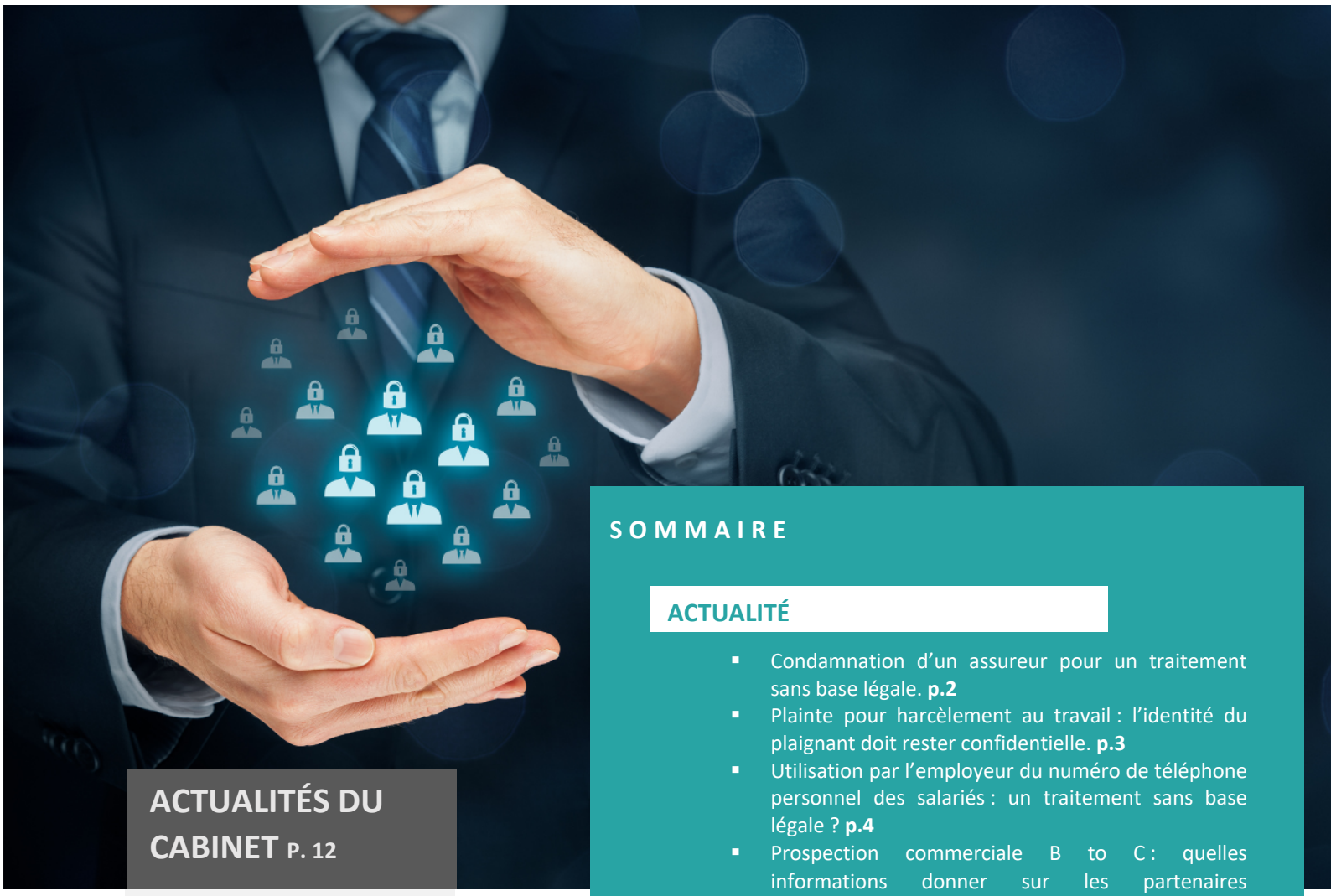
NEWSLETTER RGPD/DATA

NUMÉRO 70 ● 2025



ACTUALITÉS DU CABINET P. 12

FORMATION À LA PRÉPARATION À LA CERTIFICATION « DPO ».
DATE SUR DEMANDE

SOMMAIRE

CONDAMNATION D'UN ASSUREUR POUR UN TRAITEMENT SANS BASE LEGALE

L'autorité de contrôle espagnole a sanctionné un assureur pour s'être connecté sur une plateforme informatique au nom de ses assurés sans avoir obtenu leur consentement, quand bien même le traitement avait pour but de proposer une réduction du montant de la prime d'assurance.

Un traitement ayant pour finalité la révision à la baisse des primes d'assurance

Un assureur a pris l'initiative d'accéder à une plateforme informatique mise en œuvre par l'Etat espagnol afin de collecter les données personnelles de ses assurés.

L'objectif était de proposer à certains de ses clients une remise sur le montant de leur prime d'assurance (calculée, en l'espèce, en fonction du nombre de points sur le permis de conduire).

Pour ce faire, l'assureur avait mandaté un sous-traitant chargé d'appeler les clients afin de leur demander les informations nécessaires pour se connecter sur la plateforme (en l'occurrence, le numéro de permis de conduire et sa date de délivrance).

Un assuré, constatant que l'assureur avait accédé à ses données personnelles via la plateforme, a déposé une plainte auprès de l'autorité de contrôle espagnole.

Un traitement réalisé sans base légale

Pour sa défense, l'assureur soutenait que le traitement reposait sur la base légale de l'exécution du contrat.

L'autorité de contrôle espagnole a considéré que cette base légale n'était pas applicable en l'espèce, puisque la véritable finalité du traitement était l'octroi d'une remise sur le montant de la prime d'assurance, finalité distincte de la finalité initiale, à savoir la conclusion du contrat d'assurance.

L'assureur soutenait, subsidiairement, que le traitement reposait sur le consentement des assurés. Selon l'assureur, le contexte et les questions posées aux personnes concernées lors de l'appel téléphonique démontraient que les clients avaient consenti à ce que l'assureur se connecte sur la plateforme informatique pour, *in fine*, proposer une réduction sur le montant de la prime d'assurance.

L'autorité de contrôle espagnole a considéré que cette base légale n'était pas non plus applicable, estimant, après analyse des transcriptions des appels téléphoniques, que le consentement n'était pas suffisamment éclairé ni suffisamment univoque, dans la mesure où les informations données étaient parcellaires et qu'il n'y avait pas d'acte positif clair au traitement.

Compte tenu de ce qui précède, l'autorité de contrôle espagnole a infligé à l'assureur une amende de 300 000 €.

Source : ici

PLAINTE POUR HARCELEMENT AU TRAVAIL : L'IDENTITE DU PLAIGNANT DOIT RESTER CONFIDENTIELLE

L'autorité de contrôle espagnole a sanctionné une entreprise qui avait communiqué l'identité des plaignants aux personnes visées par la plainte.

La plainte de salariés pour harcèlement au travail et la divulgation de leur identité

En avril 2024, cinq salariés d'une entreprise ont déposé une plainte, auprès de leur CSE, pour harcèlement au travail à l'encontre de dix autres salariés.

Le CSE a alerté l'employeur et l'a enjoint d'ouvrir une enquête.

Une fois l'enquête terminée, l'employeur a transmis le rapport d'enquête non seulement au CSE, mais aussi à l'ensemble des personnes concernées par l'enquête, c'est-à-dire à la fois aux plaignants, mais également aux salariés visés par la plainte.

L'employeur a ainsi permis aux salariés faisant l'objet de l'enquête de découvrir l'identité des plaignants.

L'un des plaignants, considérant qu'il n'avait pas autorisé la divulgation de ses données personnelles aux personnes visées par sa plainte, a saisi l'autorité de contrôle espagnole.

La sanction de l'employeur pour non-respect de la confidentialité

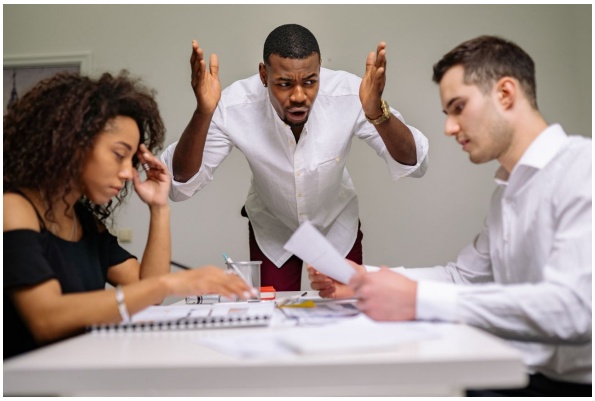
Pour sa défense, l'entreprise soutenait que l'identité des plaignants était déjà connue de l'entreprise avant même la divulgation du rapport d'enquête et que ni les plaignants ni le CSE n'avaient fait part d'une quelconque exigence de confidentialité.

L'autorité de contrôle espagnole a considéré que l'entreprise avait violé le principe d'intégrité et confidentialité posé à l'article 5§1 f) du RGPD.

En effet, selon ce principe, « *les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données* », or, en transmettant aux salariés faisant l'objet de l'enquête l'identité des plaignants, le responsable du traitement a porté atteinte à la confidentialité des données.

Compte tenu de ce qui précède, l'autorité de contrôle espagnole a infligé à l'entreprise une amende de 120 000 €.

Source : ici



UTILISATION PAR L'EMPLOYEUR DU NUMERO DE TELEPHONE PERSONNEL DES SALARIES : UN TRAITEMENT SANS BASE LEGALE ?

Par une décision du 6 mars 2025, l'autorité de contrôle espagnole a sanctionné, pour défaut de base légale, un employeur ayant traité le numéro de téléphone personnel de ses salariés pour faciliter les communications internes.

Un traitement soumis au consentement

Un salarié exerçant des fonctions de téléopérateur a saisi l'autorité de contrôle espagnole (AEPD) d'une plainte, au motif que son employeur procédait au traitement de son numéro de téléphone sans base légale.

L'enquête de l'AEPD a révélé que l'employeur avait demandé à ses salariés d'utiliser leur numéro de téléphone personnel pour communiquer avec leurs collègues de travail et leur hiérarchie via WhatsApp. Dans ce contexte, l'employeur avait diffusé, dans l'entreprise, les nom, prénom et numéro de téléphone de ses salariés.

L'employeur alléguait avoir demandé le consentement de ses salariés quant à la mise en œuvre de ce traitement et avoir proposé, en cas de refus des salariés, de communiquer par échanges de courriels.

Un traitement dépourvu de base légale

Selon l'AEPD, la base légale du consentement n'était pas envisageable en l'espèce, du fait du déséquilibre de pouvoir induit par la relation employeur/salariés (« *le consentement peut ne pas être libre dans les situations où il y a un déséquilibre de pouvoir* »).

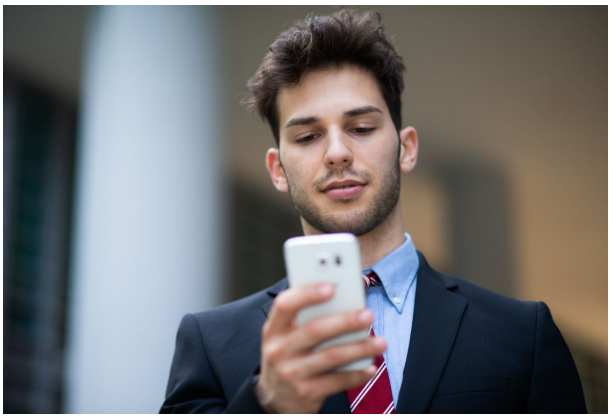
Si l'intérêt légitime était une base légale envisageable, encore fallait-il mettre en balance l'intérêt poursuivi par l'employeur et les libertés et droits fondamentaux des salariés et s'assurer que le traitement était nécessaire à la poursuite de cet intérêt :

> *« Le traitement du téléphone personnel de l'employé pourrait être fondé sur l'intérêt légitime, mais l'employeur doit procéder à une mise en balance et justifier la "nécessité" de l'utilisation du téléphone. »*

Or, en l'espèce, l'employeur n'a pas justifié de manière adéquate cette nécessité, ni de l'impossibilité d'utiliser d'autres moyens plus appropriés pour faciliter les communications internes.

Compte tenu de ce qui précède, l'AEPD a sanctionné l'employeur pour défaut de base légale au paiement d'une amende administrative de 2.000 €.

Source : ici



PROSPECTION COMMERCIALE B TO C : QUELLES INFORMATIONS DONNER SUR LES PARTENAIRES CONCERNES POUR S'ASSURER D'UN CONSENTEMENT VALABLE ?

Le Conseil d'Etat vient de saisir la Cour de Justice de l'Union européenne de questions éminemment cruciales au sujet de la transmission de données personnelles à des partenaires à des fins de prospection commerciale B to C.

Bref rappel de la position de la CNIL sur la transmission de données personnelles à des partenaires à des fins de prospection commerciale B to C

La CNIL considère que tout organisme qui entend transmettre des données personnelles à des partenaires à des fins de prospection commerciales électroniques B to C doit respecter deux séries de principes : l'information des personnes concernées, d'une part, et leur consentement, d'autre part.

Afin de s'assurer d'un consentement « éclairé »[1], l'organisme doit, selon la CNIL, être porté à la connaissance des personnes concernées « *l'identité des partenaires pour le compte desquelles le consentement est collecté et* [les] *finalités pour lesquelles les données seront utilisées* ». La CNIL va même plus loin en exigeant la mise à disposition d'une liste exhaustive et à jour des partenaires sur le formulaire de la collecte ou via un lien hypertexte[1].

L'affaire : la validité du consentement des personnes concernées à la transmission de leurs données personnelles à des partenaires pour de la prospection commerciale B to C

Le Groupe CANAL + a fait réaliser des opérations de prospection commerciale B to C, par voie électronique, auprès de millions de personnes sans avoir recueilli expressément leur consentement.

Le Groupe CANAL + avait obtenu la liste de ces personnes auprès de fournisseurs d'accès (FAI). Le formulaire de collecte utilisé par les FAI comprenait bien une case à cocher permettant de formaliser le consentement de la personne concernée à la réception de prospections commerciales par des partenaires. Toutefois, ce formulaire faisait référence aux « partenaires » des FAI, sans que ces partenaires ne soient « *nommément identifiés* » que ce soit directement dans le formulaire (via une liste accessible un lien hypertexte) ou par un autre moyen.

La CNIL, suivant sa position en la matière, a considéré que, dans de telles conditions, le consentement des personnes concernées à la transmission de leurs données à des partenaires, tels que le Groupe Canal +, pour des opérations de prospection commerciale, n'était pas éclairé et ne pouvait donc être considéré comme valablement recueilli[1]. Ce manquement (aux côtés d'autres manquements) a conduit la CNIL à sanctionner la société Groupe CANAL + (amende de 600.000 euros).

Le Groupe Canal + a formé un recours devant le Conseil d'Etat considérant que la mention de « partenaires » était suffisante.

Les questions cruciales posées à la CJUE en matière de transmission de données à des partenaires pour de la prospection B to C

Le Conseil d'Etat a décidé de soumettre à la CJUE plusieurs questions compte tenu des « *difficultés sérieuses* » que présente le sujet[1] :

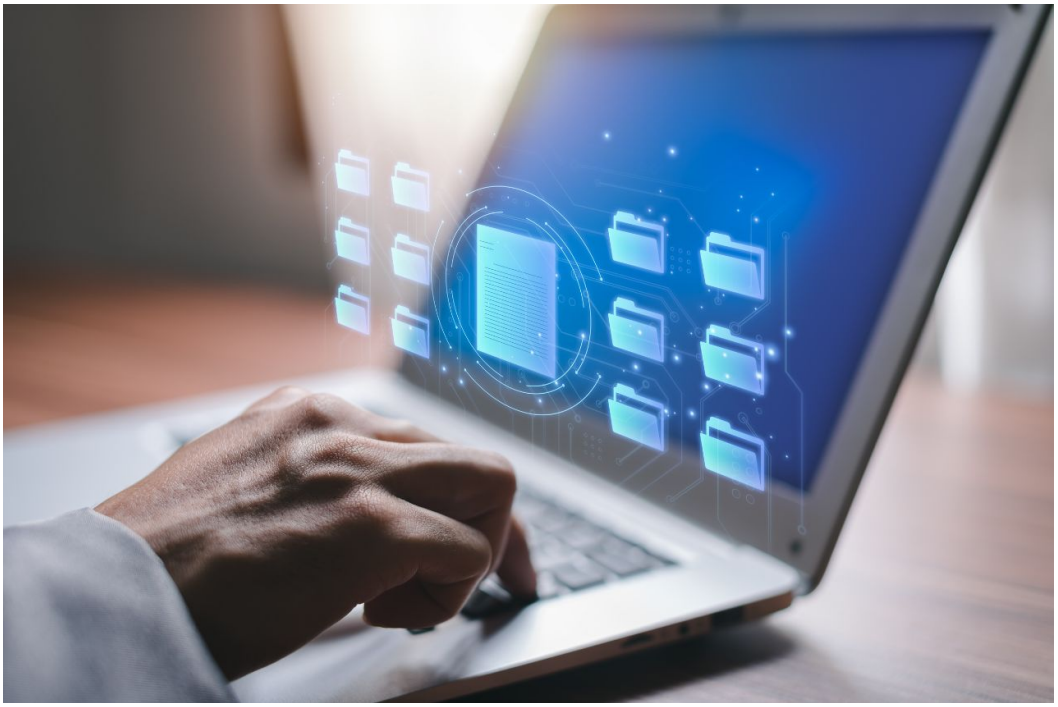
- Est-ce que le consentement d'une personne concernée à l'utilisation de ses données personnelles par une catégorie de destinataires identifiée par la mention « partenaires » peut être considéré comme un consentement valable juridiquement ?

- Quel degré de précision doit être donné sur la catégorie de destinataires ? La formule « tout partenaire » est-elle suffisante ?

La position de la CJUE est particulièrement attendue et pourrait conduire à revoir les pratiques en matière de transmission des données personnelles à des partenaires dans un but de prospection commerciale B to C.

A suivre…

[1]Cf. article 4 du RGPD.
[2]https://www.cnil.fr/fr/la-prospection-vers-les-particuliers-b-c-quelles-regles-pour-transmettre-des-donnees-des-partenaires
[3]Délibération SAN-2023-015 du 12 octobre 2023.
[4]Décision du Conseil d'Etat, 5 mai 2025, 490202.



DOCTRINE

RGPD

Fonctions du DPO : l'entreprise avait tout faux

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 différentes autorités de contrôle nationales au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question des exigences du RGPD concernant les fonctions du DPO.

La désignation d'un délégué à la protection des données (également dénommé « *Data Protection Officier* » ou « *DPO* ») est obligatoire dans les cas visés à l'article 37.1 du RGPD. Dans les autres cas, cette désignation est simplement facultative, mais largement recommandée par les autorités de contrôle et le CEPD.

Cette désignation n'est pas sans conséquence dans la mesure où elle oblige l'entreprise qui le désigne à respecter toute une série d'obligations en lien avec les fonctions du DPO (article 38 du RGPD) et ses missions (article 39 du RGPD). Ainsi, et à titre d'illustrations, l'entreprise doit : (i) veiller à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ; (ii) lui fournir les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, en lui permettant d'entretenir ses connaissances spécialisées ; (iii) veiller à ce qu'il ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions ; (iv) s'assurer qu'il fasse directement rapport au niveau le plus élevé de la direction de l'organisation dont il relève. Enfin, l'entreprise doit garantir que, si le DPO exécute d'autres missions et tâches dans l'entreprise, celles-ci n'entraînent pas de conflit d'intérêts.

L'affaire[1]

Après avoir reçu plusieurs signalements anonymes, l'autorité norvégienne de protection des données (« *Datatilsynet* ») avait lancé une mission de contrôle à l'égard de la société mère d'un groupe d'entreprises concernant le respect, par cette dernière, des exigences relatives au délégué à la protection des données. L'inspection a révélé que la société mère agissait non seulement en tant que responsable du traitement pour certaines activités de traitement, mais aussi comme sous-traitant pour le compte des filiales et parfois comme responsable conjoint du traitement avec d'autres filiales. L'équipe en charge de la protection des données était composée du DPO de la société mère et de coordinateurs de la protection de la vie privée dans les différentes sociétés du groupe et ce, afin de garantir un lien entre le DPO et les filiales.

À, la question de savoir si le DPO était associé, de manière appropriée et en temps utile, à toutes les questions relatives à la protection des données personnelles, Datatilsynet a répondu par la négative. D'abord parce qu'aucune procédure concernant le moment et la manière d'impliquer le DPO à toutes les questions relevant de son périmètre ne lui a été remise pendant l'inspection. Ensuite, parce que les investigations ont mis en

exergue que le DPO n'était associé aux questions « *RGPD* » qu'au cas par cas et que, lorsqu'il participait à des réunions relatives à ces questions, cela se faisait de manière informelle.

L'autorité norvégienne de protection des données s'est également intéressée au sujet des ressources allouées au DPO par l'entreprise. Constatant que le DPO occupait aussi un poste de juriste auquel il consacrait 50% de son temps, Datatilsynet a estimé que l'attribution d'un demi ETP pour la fonction dédiée à la protection des données était insuffisante. Pour en arriver à cette conclusion, l'autorité s'est notamment appuyée sur des notes internes indiquant que le DPO ne disposait pas de suffisamment de temps pour accomplir ses missions et que, la majeure partie de celui-ci, il se consacrait à « *la gestion rétroactive des problèmes, au lieu d'un travail proactif et stratégique* ».

Autre manquement constaté par Datatilsynet, le DPO ne faisait pas un rapport au plus haut niveau de direction de la société mère qui l'avait désigné. Si la description du poste mentionnait une telle exigence, l'autorité de protection des données a relevé qu'une telle formulation « *ne démontre pas l'existence d'une relation directe entre le DPO et le plus haut niveau de direction* », étant précisé que le conseil d'administration était « *officiellement* » le plus haut niveau de la société mère. Or, le DPO rendait des comptes non pas à cet organe mais au vice-président exécutif, au directeur des ressources humaines et du développement durable et au comité de conformité.

Enfin, l'autorité norvégienne de protection des données a estimé que la société mère n'avait pas procédé à toutes les évaluations qu'elle aurait dû faire concernant l'indépendance du DPO et que la distinction entre les rôles et les tâches du DPO et du juriste n'était pas suffisamment claire. « *Nous soulignons que le fait de travailler en tant que juriste n'exclut pas en soi la possibilité d'exercer les fonctions de DPO, par exemple si les conseils juridiques portent sur des domaines du droit autres que la protection des données* », a souligné l'autorité. En l'espèce, le contrôleur a relevé que le manque de clarté concernant ces deux activités était accentué par le fait que le DPO n'utilisait pas une messagerie électronique distincte selon ses activités et que sa signature électronique mentionnait ses deux rôles : « *Juriste associé et délégué à la protection des données* ». Ainsi, « *un collègue qui recevait un courriel contenant des conseils en matière de protection des données de la part du DPO était incapable de distinguer si les conseils provenaient de la fonction de DPO ou de la fonction de juriste* », en a conclu Datatilsynet.

Quelles recommandations ?

Il est fondamental de reprendre les exigences du RGPD dans la lettre de mission du DPO et dans des procédures internes, mais il convient aussi et surtout de mener une réflexion sur les conditions dans lesquelles ces exigences sont effectivement déployées dans l'entreprise. Cette réflexion doit se traduire par des notes internes et des procédures expliquant les règles en vigueur visant à garantir que les fonctions du DPO sont respectées.

Alexandre FIEVEE
Avocat Associé
DERRIENNIC ASSOCIES

Notes

(1) Datatilsynet, 21/03823-45, 10 mars 2025.

VU DANS LA PRESSE

« DSIH », MAI 2025

UN HOPITAL, SOUS-TRAITANT, SANCTIONNE POUR NE PAS AVOIR DECLARE LES SOUS-TRAITANTS

Par décision du 10 avril 2025 [1], l'autorité de contrôle espagnole a infligé une amende de 500.000 euros à un hôpital qui avait recruté des sous-traitants ultérieurs sans en informer préalablement le responsable du traitement.

Un sous-traitant bénéficiant d'une autorisation générale de recruter des sous-traitants ultérieurs

Le ministère de la santé de Valence a eu recours aux services de l'hôpital Marina Salud, aux termes d'un contrat relatif à la fourniture de services de soins de santé. L'hôpital, qualifié dans le contrat de « sous-traitant » au sens du RGPD (ce qui est assez étonnant), bénéficiait d'une autorisation générale de recruter des sous-traitants ultérieurs, sous réserve d'en informer préalablement le ministère de la santé.

Au cours d'un audit réalisé auprès de l'hôpital, le ministère de la santé a constaté que son sous-traitant utilisait des logiciels tiers pour réaliser certains traitements qui lui étaient confiés, suggérant que l'hôpital avait recruté des sous-traitants ultérieurs à l'insu du ministère de la santé.

À la suite du refus de l'hôpital de communiquer les contrats des fournisseurs des logiciels tiers, le ministère de la santé de Valence a saisi l'autorité de contrôle espagnole (AEPD) d'une plainte.

L'autorisation générale de recruter des sous-traitants ne dispense pas le sous-traitant de son obligation d'informer le responsable du traitement

L'enquête menée par l'AEPD a mis en lumière que l'hôpital avait, dans le cadre des traitements réalisés pour le compte du ministère de la santé, eu recours à des sous-traitants ultérieurs, dont l'identité n'avait pas été communiquée au ministère de la santé.

Or, le contrat conclu avec le ministère de la santé, s'il instaurait une autorisation générale de recourir à des sous-traitants, assortissait cette autorisation d'une obligation de porter à la connaissance du ministère de la santé l'identité des sous-traitants auquel l'hôpital avait recours.

De même, l'article 28 du RGPD prévoit qu'en cas d'autorisation générale de sous-traitance ultérieure, il appartient au sous-traitant d'informer le responsable du traitement de « *tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitant* » et ce, afin de donner à ce dernier la possibilité d'émettre des objections à l'encontre de ces changements.

Compte tenu de ce qui précède, l'AEPD a considéré que l'hôpital avait non seulement violé le contrat conclu avec le ministère de la santé, mais avait aussi manqué à ses obligations au titre de l'article 28 du RGPD.

A noter enfin que, selon l'AEPD, le défaut d'information du responsable du traitement est une violation continue, qui persiste pendant toute la durée du recours au sous-traitant ultérieur à l'insu du responsable du traitement. La durée de cette violation a été prise en compte par l'AEPD, qui a fixé le montant de l'amende à 500.000 euros.

Alexandre Fievée

Gaétan Dufoulon

Alice Robert

1https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202307719

VU DANS LA PRESSE

« DSIH », AVRIL 2025

PSEUDONYMISATION DES DONNEES DE SANTE PERSONNELLES : DE NOUVELLES CLARIFICATIONS

La pseudonymisation des données de santé personnelles est une technique requise, dans certains cas, pour assurer la conformité légale de vos traitements. Elle soulève toutefois des questions quant à sa caractérisation et sa mise en œuvre. De nouvelles lignes directrices du CEPD ont récemment été publiées sur le sujet[1].

Dans le secteur de la santé, le recours à des données pseudonymisées peut être nécessaire dans le cadre de certains traitements de données de santé à caractère personnel. Plusieurs « référentiels CNIL » imposent d'ailleurs, dans des cas spécifiques, le recours à la pseudonymisation. A titre d'exemple, le référentiel sur l'EDS impose la pseudonymisation des données de santé à caractère personnel comme une exigence de sécurité à plusieurs niveaux.

Mais qu'entend-on par pseudonymisation ? Quel est l'intérêt de recourir à une telle technique et comment la mettre en œuvre ?

Le Comité Européen à la Protection des Données (CEPD ou EDPB) a récemment adopté, des lignes directrices apportant quelques clarifications à ces questions.

La pseudonymisation, de quoi parle-t-on ?

Le CEPD rappelle que la pseudonymisation est un « *traitement de données à caractère personnel de telle sorte que ces données ne puissent plus être attribuées à une personne concernée précise sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* »[2].

Concrètement, la pseudonymisation consiste à remplacer des données à caractère personnel directement identifiantes (exemples : nom, prénom, adresse, numéro de téléphone) par des données indirectement identifiantes (exemples : alias, codes) – les « données pseudonymisées » -, étant précisé que, pour pouvoir réidentifier la personne concernée par les données pseudonymisées, il faut disposer d'informations supplémentaires, telles que, comme l'indique le CEPD, un tableau de correspondance ou encore des clés cryptographiques. Le CEPD souligne le fait que ces informations supplémentaires – qui permettent donc d'identifier directement la personne concernée – ne doivent pas être divulguées ou utilisées par les personnes qui traitent les données pseudonymisées.

Les données pseudonymisées sont des données à caractère personnel, comme le rappelle le CEPD. Toutefois, le CEPD indique que « *si les données pseudonymisées et les informations complémentaires peuvent être combinées compte tenu des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par une autre personne, les données pseudonymisées sont alors à caractère personnel* ».

Pourquoi une telle précision ? Y aurait-il des données pseudonymisées qui ne seraient pas à caractère personnel ? Est-ce que cette précision vient faire écho à la position prise par le Tribunal de l'Union Européenne (TUE) dans une affaire de 2023 et, plus récemment, par l'Avocat général près la Cour de Justice de l'Union européenne (CJUE) ? Le TUE a jugé que, pour déterminer si les informations transmises au tiers sont « *des informations se rapportant à "une personne physique identifiable"* », il convient de rechercher si ce tiers dispose « *de moyens légaux et réalisables en pratique lui permettant d'accéder aux informations supplémentaires nécessaires à la réidentification des auteurs des commentaires* »[3].

À défaut, les informations transmises ne sont pas des données à caractère personnel. L'Avocat général a adopté une approche similaire, considérant que le tiers ne doit être considéré comme traitant des données personnelles que sous réserve qu'il dispose *« de moyens raisonnables d'identifier* [les personnes concernées][4] ».

Pourquoi recourir à la pseudonymisation dans le secteur de la santé et comment ?

Le CEPD prend l'exemple d'un hôpital universitaire qui chercherait à améliorer ses services et ses processus de facturation. Pour ce faire, l'hôpital aurait besoin d'analyser des données de « traitement » (durée du séjour, procédures de diagnostic et interventions thérapeutiques appliquées, ressources consacrées aux soins du patient, données d'identification du patient, etc.). L'hôpital se trouverait alors confronté à la problématique suivante : permettre à son personnel administratif non médical travaillant dans « *un environnement de sécurité moyen* » une analyse de données médicales particulièrement sensibles, tout en étant en capacité de pouvoir remonter des informations aux gestionnaires de soins au cas où des irrégularités seraient constatées dans les données.

Selon le CEPD, l'hôpital pourrait recourir à la pseudonymisation afin que son personnel administratif non médical n'ait pas accès aux données de « traitement » identifiant les patients.

Le CEPD propose alors un processus de mise en œuvre d'une telle pseudonymisation.

Il s'agirait, dans un premier temps, de sélectionner les données pertinentes pour l'analyse à réaliser (ex. : durée du séjour, diagnostics, etc.), à l'exclusion (i) des « *documents très individuels* » (ex. : lettre de sortie), (ii) des documents présentant un risque particulier de confidentialité (ex. : notoriété d'un dossier, intérêt pour le public du patient, etc.) et (iii) des données permettant au personnel extérieur aux départements médicaux d'identifier directement les patients.

Dans un deuxième temps, ces données pertinentes sélectionnées, ainsi que l'identifiant du patient et l'ID du dossier cryptés, seraient transmis à une base de données dédiée « *opérant en dehors de la zone du réseau médical* ». Quant aux informations supplémentaires nécessaires à l'identification des patients (clé de chiffrement, dossiers médicaux originaux), elles seraient stockées dans une autre base. L'analyse serait alors faite, dans un dernier temps, exclusivement sur les données figurant dans la base pseudonymisée dédiée, étant précisé que seul le personnel non médical n'ayant pas accès au SI de l'hôpital aurait un accès à cette base.

La pseudonymisation apparaît ici notamment comme une mesure de sécurité dans la mesure où la personne accédant à la base de données dédiée, sans autorisation et sans connaissance préalable de l'état de santé des patients sélectionnés, ne serait pas en mesure de tirer des conclusions sur l'état de santé d'un individu.

Si la pseudonymisaiton des données de santé reste un sujet épineux, ces nouvelles lignes directrices du CEPD constituent un nouveau document de référence à prendre en compte.

[1]https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf

[2]Article 4(5) du RGPD.

[3]TUE26 avril 2023 (aff. T-5, 57/20).

[4]Conclusions de l'Avocat général, M. Spielmann ? – 6 février 2025 (aff. C-413/23 P).

Alexandre Fievée et Alice Robert

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

4.000 € 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* » (2024).

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

Enfin, en 2025, il fait son entrée dans le classement Chambers France, se positionnant en Band 3 dans le classement individuel Data Protection.

RENSEIGNEMENTS PRATIQUES

Prochaine session en 2025 :
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