NEWSLETTER RGPD/DATA

NUMÉRO 50

ACTUALITES DU CABINET

24 JANVIER –
Trophée d'argent « Données personnelles et Cybersécurité » P. 2

8 MARS 2023 -
MATINALE « *Action répressive de la CNIL : quel bilan pour 2022 ?* » P. 2

DATE SUR DEMANDE
FORMATION A LA PREPARATION A LA CERTIFICATION « DPO ». P. 13

SOMMAIRE

ACTUALITÉS DU CABINET

RECOMPENSE DU CABINET 2023

Cette année le cabinet Derriennic a été distingué « Trophée d'argent » dans la catégorie « Données personnelles et Cybersécurité » au Sommet du droit 2023.

PROCHAINE MATINALE

ACTUALITE

COOKIES : SANCTION DE MICROSOFT POUR NON-RESPECT DES REGLES DE RECUEIL DU CONSENTEMENT

Le 19 décembre 2022, la CNIL a prononcé une amende de 60 millions d'euros à l'encontre de Microsoft pour avoir manqué à l'obligation de recueil du consentement en matière de cookies et pour ne pas avoir mis en place, sur le moteur de recherche « Bing », un système permettant de refuser les cookies aussi simplement que de les accepter.

A la suite d'une plainte déposée par un utilisateur considérant que les « *conditions de recueil du consentement au dépôt de cookies* » sur le moteur de recherche « Bing » n'étaient pas conformes à la réglementation, la CNIL a ouvert une enquête à l'encontre de Microsoft, titulaire dudit moteur de recherche.

Au cours de cette enquête, l'autorité de contrôle a relevé deux manquements aux obligations en matière de cookies posées à l'article 82 de la Loi Informatique et Libertés (ci-après « LIL ») :

1. Manquement à l'obligation de recueil du consentement lors du dépôt d'un cookie non-« essentiel »

La CNIL a d'abord constaté que, dès l'arrivée de l'internaute sur le moteur de recherche « Bing », un cookie « *multi-finalités* » était automatiquement déposé sur le terminal de l'utilisateur sans son consentement.

Pour mémoire, les cookies « *multi-finalités* » sont une « *souplesse* » accordée aux responsables du traitement qui leur permettent de regrouper plusieurs finalités dans un seul et même cookie afin de ne « *pas surcharger le terminal de l'utilisateur* » en déposant une multitude de cookies ayant des finalités distinctes.

Pour la CNIL, « *si un cookie multi-finalités peut être déposé sans consentement pour une finalité essentielle, [le responsable du traitement] ne peut utiliser ce cookie pour des finalités non-essentielles que si l'utilisateur a effectivement consenti à ces finalités spécifiques* ».

Pour rappel, un cookie ayant une finalité « *essentielle* » est un cookie « *qui relève de l'une des deux exemptions prévues à l'article 82 de la LIL* », autrement dit un cookie (i) qui « *permet ou facilite la communication par voie électronique* » ou (ii) qui est « *strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur* ».

En l'espèce, l'autorité de contrôle a considéré que l'une des finalités du cookie « *multi-finalités* » déposé par Microsoft, à savoir « *la détection et le filtrage des fraudes publicitaires* », n'était pas une finalité « *essentielle* » et que, en conséquence, Microsoft aurait dû obtenir le consentement de l'utilisateur avant de pouvoir utiliser ce cookie pour une telle finalité. En ne sollicitant pas préalablement le consentement de l'internaute, la CNIL a estimé que Microsoft avait méconnu les obligations de l'article 82 de la LIL.

L'autorité de contrôle a ensuite constaté qu'un cookie à finalité publicitaire était déposé sur le terminal de l'utilisateur lors de la navigation, et ce, toujours sans le consentement de ce dernier. Microsoft a indiqué que « *ce cookie avait été ajouté par inadvertance* ».

Selon la CNIL, « *si le dépôt du cookie sans recueillir le consentement de l'utilisateur n'était pas intentionnel, il résultait néanmoins d'une erreur grossière de la part de la société qui n'a pas contesté la finalité publicitaire dudit cookie (…)* ».

Ici encore, l'autorité de contrôle a considéré que Microsoft a méconnu les dispositions de l'article 82 de la LIL.

2. Manquement à l'obligation d'équilibre entre les modalités d'acceptation et de refus des cookies

La CNIL a enfin constaté que le « *bandeau cookies* » affiché sur le moteur de recherche « Bing » proposait un bouton permettant d'accepter directement les cookies, mais ne proposait aucun moyen analogue permettant de refuser « *facilement et en un seul clic* » lesdits cookies. Effectivement, deux clics étaient nécessaires pour les refuser, alors qu'un seul suffisait à les accepter.

L'autorité de contrôle a rappelé la nécessité d'un « *équilibre entre les modalités d'acceptation et de refus* ». En l'espèce, le site faisait apparaître une « *fenêtre surgissante présentant un bouton "Accepter" et un bouton "Plus d'options"* ».

La CNIL a considéré que le bouton "*Plus d'options*" n'était pas explicite, et que « *le fait de rendre le mécanisme de refus des cookies plus complexe que celui consistant à les accepter revient en réalité à décourager les utilisateurs de refuser les cookies et à les inciter à privilégier la facilité du bouton "Accepter"* ».

En conséquence, l'autorité de contrôle a considéré que le « *bandeau cookies* » de « Bing » n'était pas conforme aux dispositions de l'article 82 de la LIL.

Compte tenu de ce qui précède, la CNIL (i) a prononcé une amende administrative de 60 millions d'euros à l'encontre de Microsoft pour les multiples violations de l'article 82 de la LIL, et (ii) a enjoint à Microsoft, dans un délai de trois mois, de recueillir le consentement des utilisateurs du moteur de recherche « Bing » avant tout dépôt de cookies non-essentiels.

Source : ici

L'AUTORITE IRLANDAISE CONTRAINTE A CONDAMNER META A 390 MILLIONS D'EUROS D'AMENDE

Suite à un désaccord entre plusieurs autorités de contrôle européenne, le Comité européen à la protection des données (CEPD) a rédigé trois décisions contraignantes, concernant Facebook, Instagram et WhatsApp, que l'autorité de contrôle irlandaise a été amenée à prononcer.

L'autorité de contrôle irlandaise (la *Data Protection Commission*, ou « DPC ») a reçu, le jour de l'entrée en application du RGPD, des plaintes de citoyens autrichiens et belges concernant Facebook et Instagram.

Ces plaintes faisaient état de la mise en œuvre de publicités ciblées via les services de Facebook et d'Instagram, sans que le consentement des utilisateurs ne soit recueilli.

Ces plaintes ont conduit la DPC à rédiger un projet de décision, prévoyant la sanction de Meta au titre du défaut de transparence. En effet, pour la DPC, les utilisateurs n'étaient pas informés de façon suffisamment claire quant aux opérations de traitement qui étaient réalisées sur leurs données personnelles, ni sur les finalités de traitement et les bases légales. En revanche, la DPC a considéré que les traitements liés à la publicité ciblée pouvaient reposer, comme le prévoyait Meta, sur la base légale de l'exécution contractuelles et n'avaient pas à s'appuyer sur le consentement des utilisateurs.

Ce projet de décision a été soumis à l'ensemble des autorités de contrôle européennes, dont certaines, à l'instar de la CNIL, ont considéré :

- que le montant de la sanction proposée par la DPC était trop bas ;
- que les traitements liés à la publicité ciblée ne pouvaient pas reposer sur la base légale de l'exécution contractuelle, mais bel et bien sur celle du consentement ;

La DPC ayant maintenu sa position et devant l'impossibilité d'atteindre un consensus, le CEPD est intervenu et, aux termes de plusieurs décisions contraignantes, a considéré que Meta ne pouvait pas s'appuyer sur la base légale de l'exécution contractuelle et que le montant de l'amende devait être revu à la hausse.

Dans ce contexte, la DPC s'est alignée sur les conclusions du CEPD et a augmenté le montant des amendes (210.000.000 € s'agissant de Facebook et 180.000.000 € s'agissant d'Instagram).

Source : ici

DROIT D'ACCES : PRECISIONS DE LA CJUE SUR LES INFORMATIONS RELATIVES AUX DESTINATAIRES DES DONNEES PERSONNELLES

Dans un arrêt rendu le 12 janvier dernier, la CJUE a tranché l'épineuse question de savoir si le responsable de traitement doit, dans le cadre d'une demande de droit d'accès, communiquer l'identité exacte des destinataires des données qu'il traite ou bien seulement les catégories de ces destinataires.

Selon l'article 15 1. b) du RGPD, la personne concernée peut avoir accès à plusieurs informations dont celles concernant « *les destinataires ou catégories de destinataires* » auxquels les données le concernant ont été communiquées.

Au visa de cet article, un citoyen autrichien a demandé à un opérateur de services postaux et logistiques de lui communiquer l'identité des destinataires auxquels ledit opérateur avait transmis ses données personnelles.

L'opérateur s'étant contenté de lui communiquer les catégories de destinataires, le citoyen a saisi la juridiction autrichienne pour obtenir l'identité exacte desdits destinataires.

La juridiction autrichienne a alors interrogé la CJUE sur le point de savoir si le RGPD laisse au responsable de traitement le libre choix de communiquer (i) l'identité des destinataires ou (ii) seulement les catégories de destinataires.

La CJUE a adopté une position claire : le responsable de traitement à l'obligation de fournir à la personne concernée l'identité même des destinataires auxquelles des données à caractère personnel la concernant sont communiquées.

La CJUE apporte, toutefois, deux exceptions à cette obligation :

1. Si le responsable de traitement ne peut pas (ou pas encore) identifier les destinataires, seules les catégories de destinataires peuvent être indiquées ;

2. Si la demande est manifestement infondée ou excessive.

Pour justifier une telle solution, les juges européens ont notamment souligné que le droit d'accès est nécessaire pour l'exercice d'autres droits par la personne concernée (droit d'opposition, droit à la limitation, droit de recours, etc.).

Tout responsable de traitement doit donc être particulièrement vigilant dans la réponse à apporter aux demandes de droits d'accès, les informations sur les destinataires de données devant, par principe, être plus précises (identité concrète des destinataires) que celles devant être fournies pour respecter l'obligation d'information prévues par les articles 13 et 14 du RGPD (pouvant se limiter, par principe, aux catégories des destinataires).

Source : ici

PUBLICITES PERSONNALISEES PAR DEFAUT : SANCTION DE LA SOCIETE APPLE

Par une délibération du 29 décembre 2022, la CNIL a prononcé une amende de 8 millions d'euros à l'encontre de la société Apple pour avoir activé, par défaut, les « Publicités personnalisées » sur ses systèmes d'exploitation.

Le 10 mars 2021, l'association FRANCE DIGITALE a saisi la CNIL d'une plainte à l'encontre de la société APPLE concernant les traitements mis en œuvre au travers de ses systèmes d'exploitation.

FRANCE DIGITALE reprochait à la société APPLE d'avoir activé par défaut les *« Publicités personnalisées »* et, ce faisant, de ne « *pas permettre aux utilisateurs de consentir valablement aux traitements de ciblage publicitaire* ».

Au cours de son enquête, et après avoir établi sa compétence matérielle et territoriale, la CNIL a constaté que « *dans la rubrique intitulée "Publicité Apple", […] les paramètres de ciblage de la publicité sont pré-cochés par défaut ».*

Entrant dans le détail technique, la CNIL a considéré que pour effectuer son ciblage publicitaire, la société APPLE procédait à des « *opérations de lecture et/ou d'écriture d'informations sur les terminaux des utilisateurs* », entraînant de ce fait « *l'application de l'article 82 de la loi informatique et libertés* ».

En conséquence, la CNIL a considéré que *« les traitements de ciblage de la publicité ne sauraient être considérés comme ayant été acceptés par un acte positif des utilisateurs* » et donc que la société APPLE a agi en méconnaissance des dispositions de l'article 82 de la loi Informatique et Libertés.

Parallèlement, l'autorité de contrôle a reproché à la société APPLE un recueil tardif du consentement. Effectivement, la possibilité de désactiver les « *Publicités personnalisées* » n'est accessible qu'après que l'utilisateur ait cliqué sur l'icône « *Réglages* » de l'iPhone, se soit rendu dans le menu « *Confidentialité* », puis ait cliqué sur la rubrique intitulée « *Publicité Apple* ».

Elle estime également qu'il est difficile pour l'utilisateur de parvenir à accepter ou refuser valablement ces opérations, dans la mesure où l'utilisateur, qui a terminé le parcours d'initialisation de son téléphone, peut légitimement penser ne plus avoir besoin de procéder à d'autres configurations.

Compte tenu de ce qui précède, sans préjudice du fait que ce manquement ait été corrigé dans les versions ultérieures des systèmes d'exploitation de la société APPLE, la CNIL a infligé à cette dernière une amende de 8 millions d'euros.

Source : ici

DOCTRINE

RGPD

Le DPO : dans l'œil du cyclone ?

(Seconde partie)

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. Le mois dernier, il s'est penché sur la question des fonctions du DPO, et plus particulièrement celle de son positionnement dans l'organisme (Première partie). Ce mois-ci, il aborde la problématique de l'exercice effectif par le DPO de ses missions.

Le CEPD (Comité européen à la protection des données) a annoncé, en septembre dernier, que son action coordonnée 2022/2023 portera sur les problématiques liées à la désignation du DPO, son positionnement dans les organismes et ses missions. Dans le cadre de cette action coordonnée, le CEPD a invité les autorités nationales de protection des données à travailler sur le sujet.
Jusqu'à présent, l'action « *répressive* » de la Cnil sur la question du DPO -son positionnement dans al'organisme, ses ressources, ses missions- est restée relativement limitée. Faut-il s'attendre à ce que la Cnil diligente des missions de contrôle sur ce sujet ?

A l'aide de plusieurs décisions d'autorités de contrôle d'autres pays européens, nous allons essayer d'identifier – à partir des manquements constatés – les principales zones de risques. Ce mois-ci, nous allons aborder trois problématiques : la mission d'information et de conseil du DPO, ses missions de contrôle et la question de la planification de ses actions en fonction du risque.

En effet, il ressort des termes de l'article 39-1 du RGPD que le DPO a notamment pour mission d'informer et de conseiller le responsable du traitement (ou le sous-traitant) ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la règlementation ; de contrôler le respect du RGPD par l'organisme dont il dépend ; et de dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et de vérifier l'exécution de celle-ci. L'article 39-2 du RGPD ajoute que le DPO tient dûment compte, dans l'accomplissement de ses missions, « *du risque associé aux opérations de traitement* » compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Les affaires

Dans plusieurs décisions rendues par les autorités luxembourgeoise (la « *CNPD* ») et hollandaise (« *l'AP* »), des organismes ont été sanctionnés pour ne pas avoir permis au DPO d'exercer ses missions d'information et de conseil. Tel a été le cas d'une société qui ne permettait pas à son délégué à la protection des données de réaliser un reporting formel et spécifique de son activité à l'encadrement supérieur, quand bien même des points réguliers étaient organisés. L'autorité luxembourgeoise a en effet considéré que, dès lors que la mission d'information et de conseil l'égard du responsable du traitement est « *intimement liée* » à l'obligation d'associer le DPO de manière appropriée et en temps utile à toutes les questions relatives à la protection des données, l'organisme avait manqué à ses obligations[1].

L'autorité hollandaise a adopté une position identique : « *Il est important que le responsable du traitement veille à ce que le DPO soit associé de manière appropriée et en temps utile à toutes les questions liées à la protection des données à caractère personnel. L'AP a établi que l'Administration fiscale et douanière n'avait pas correctement et en temps voulu associé le DPO pour mettre en œuvre une analyse d'impact (...). Il en résulte que le DPO n'a pas été en mesure d'accomplir correctement ses tâches et n'a donc pas été en mesure de conseiller à temps les autorités fiscales sur le respect du RGPD. En cas de consultation en temps opportun, le DPO aurait pu avertir plus tôt l'administration fiscale et douanière des risques associés au traitement inapproprié des données personnelles (...).* »[2]

Dans d'autres affaires, ce n'est pas le caractère effectif de la mission d'information et de conseil qui posait difficulté, mais les conditions dans lesquelles la mission de contrôle était réalisée par le DPO. Si la CNPD reconnaît que l'article 39.1 du RGPD n'impose pas à l'organisme de mette en place des mesures spécifiques pour assurer que le DPO accomplit sa mission de contrôle et que la tenue du registre des activités de traitement contribue à l'exercice de cette mission, elle relève toutefois que « *cet élément [la tenue du registre] pris isolément ne suffit pas à démontrer que la mission de contrôle du respect du RGPD est effectuée de manière adéquate* »[3].

Ainsi, selon l'autorité luxembourgeoise, « *la mission de contrôle effectuée par le DPO auprès du contrôlé devrait être suffisamment formalisée, par exemple par un plan de contrôle en matière de protection des données, afin de pouvoir démontrer que le DPO effectue sa mission de contrôle du respect du RGPD de manière adéquate.* » La CNPD a repris cette solution dans plusieurs autres affaires[4].

Enfin, dans une décision rendue par l'autorité polonaise de protection des données (« *UOPO* »), un éclairage est donné sur les attentes concernant l'article 39-2 du RGPD, selon lequel le DPO doit accomplir ses missions en tenant compte des « *risques* » liés aux opérations de traitement. Selon l'UODO : « *Cette disposition impose au délégué de fixer des priorités dans son travail, qui devrait consister à déterminer de manière individuelle et indépendante des mesures et des modalités de fonctionnement et à les adapter à la spécificité de l'organisme. Dans ce contexte, il est important d'identifier au préalable les risques liés au traitement des données personnelles et, sur cette base, de déterminer des solutions efficaces, tant techniques qu'organisationnelles. Il s'agit d'une approche sélective et pragmatique. Se concentrer sur les aspects qui comportent des risques plus élevés pour la protection des données à caractère personnel devrait permettre au DPO de conseiller plus facilement le responsable du traitement sur la méthodologie à utiliser lors de la réalisation du DPIA, sur les domaines devant être audités en interne ou en externe, sur les formations internes à planifier et réaliser pour les employés (...).* »[5]

Quelles recommandations ?

Organiser la participation directe, systématique et en temps utile du DPO aux différents comités dans lesquels sont discutées des questions portant sur la protection des données personnelles et donner à celui-ci un accès direct et non conditionné au niveau le plus élevé de la direction, semblent être des prérequis incontournables pour permettre au DPO d'exercer de manière effective ses missions d'information et de conseil.

Par ailleurs, il semble indispensable que l'organisme vérifie la mise en place par le DPO d'un plan d'actions comportant, parmi les actions à déployer, un plan de contrôle visant à vérifier que les préconisations qu'il a formulées ont bien été implémentées. A cet égard, il appartient au DPO de concevoir son plan d'actions selon une approche reposant sur le risque, c'est-à-dire en priorisant ses interventions et les mesures techniques et organisationnelles à mettre en œuvre en fonction des niveaux de risques identifiés.

Alexandre FIEVEE
Avocat Associé
DERRIENNIC ASSOCIES

Notes

(1) CNPD, Délibération n° 18FR/2021, 31 mai 2021.

(2) AP, Décision, 7 avril 2022.

(3) CNPD, Délibération n° 36FR/2021, 13 octobre 2021.

(4) CNPD, Délibération n° 38FR/2021, 15 octobre 2021 ; CNPD, Délibération n° 40FR/2021, 27 octobre 2021.

(5) UODO, Décision, 21 août 2020.

PANORAMA EUROPÉEN

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

Illicéité de l'accès aux courriels d'un ancien salarié

Personvernnmemnda (Norvège), 13 décembre 2022

L'autorité de contrôle norvégienne a sanctionné un employeur pour avoir mis en place un transfert automatique des courriels d'un ancien salarié sans l'en informer.

A la suite de la démission d'un salarié, un transfert automatique de tous les courriels de celui-ci a été mis en place vers la boite aux lettres électronique du directeur général de l'entreprise pour une durée de 6 semaines.

Ayant appris l'existence d'un tel dispositif, le salarié a exercé son droit d'opposition puis s'est plaint auprès de l'autorité de contrôle norvégienne.

Au cours de son enquête, cette dernière a reproché à l'employeur :

- De n'avoir pas informé le salarié de l'existence d'un tel transfert de courriel ;
- De ne pas avoir répondu favorablement à l'exercice, par le salarié, de son droit d'opposition.

Rappelant que « *la surveillance continue des courriels d'un salarié [est une] ingérence grave dans le droit de l'employé à correspondre librement [ainsi qu'une] atteinte à la vie privée des tiers qui ont envoyé des courriels à l'employé* », l'autorité de contrôle a prononcé une amende d'environ 9.300 € à l'encontre de l'employeur.

Source : ici

Communication illicite de l'employeur

Datatilsynet (Danemark), 2 décembre 2022

L'autorité de contrôle danoise a sanctionné un employeur qui a informé ses clients du licenciement d'un de ses salariés ayant commis des infractions pénales dans le cadre de l'exercice de ses fonctions.

Un employeur a informé plusieurs de ses clients, par courrier électronique, qu'un de ses employés avait commis des infractions pénales dans le cadre de l'exercice de ses fonctions et avait donc, pour ce motif, été licencié.

Ce dernier a déposé une plainte auprès de l'autorité de contrôle danoise, considérant que ces informations avaient été transmises à des tiers sans son consentement et de manière illicite.

Au cours de son enquête, l'autorité de contrôle a effectué une mise en balance entre (i) l'intérêt légitime de l'entreprise à transmettre à ses clients des informations sur le licenciement d'un salarié, et (ii) l'intérêt du salarié au maintien de la confidentialité d'informations le concernant.

L'autorité relève que l'employeur avait un intérêt légitime à informer ses clients du licenciement d'un salarié, notamment pour les informer qu'il ne peut plus conclure de contrats au nom de l'entreprise. En revanche, l'autorité retient que la fourniture de « *descriptions plus détaillées des allégations à l'encontre de l'ancien employé* » n'était « *pas nécessaire pour atteindre cet objectif* », d'autant que les données à caractère personnel relatives à des condamnations pénales et à des infractions sont des données sensibles, en application du RGPD.

L'autorité de contrôle danoise a infligé une amende d'environ 20.000 euros à l'employeur.

Source : ici

Sanction d'une agence immobilière pour n'avoir pas retiré l'annonce d'un bien immobilier déjà vendu

APD (Belgique), 24 novembre 2022

L'autorité de contrôle belge a prononcé un avertissement à l'encontre d'une agence immobilière qui, après la vente d'un bien immobilier, a laissé l'annonce sur son site en dépit de l'exercice, par le nouvel acquéreur, de ses droits à l'effacement et d'opposition.

Malgré la vente d'un bien immobilier, une agence immobilière avait laissé l'annonce du bien, mentionnant l'adresse et le numéro de parcelle cadastrale, sur son site internet.

Le nouveau propriétaire du bien immobilier exerça ses droits à l'effacement et d'opposition afin que l'annonce soit retirée, mais l'agence refusa de faire droit à ces demandes au motif que l'annonce poursuivait des finalités de « *marketing de son activité commerciale d'agent* ». Face à ce refus, l'acquéreur déposa une plainte auprès de l'autorité de contrôle belge.

Au cours de son enquête, cette dernière a d'abord considéré que la publication des images d'une maison, accompagnée de l'adresse postale et du numéro de parcelle cadastrale, était constitutive d'un traitement de données à caractère personnel.

Partant de ce constat, l'autorité de contrôle a cherché à identifier la base légale d'un tel traitement.

Rappelant qu'une agence immobilière peut fonder la licéité de son traitement sur l'exécution d'un contrat, l'autorité de contrôle a considéré que cette base légale n'était pas applicable en l'espèce puisque l'acheteur n'était pas partie au contrat existant entre l'agence immobilière et le vendeur.

L'autorité de contrôle a rappelé, dans un second temps, que l'utilisation de l'intérêt légitime comme base légale suppose la démonstration des éléments suivants :

> *« 1) les intérêts qu'il poursuit avec le traitement peuvent être reconnus comme légitimes (le « test de finalité ») ;*
>
> *2) le traitement envisagé est nécessaire pour réaliser ces intérêts (le « test de nécessité ») ; et,*
>
> *3) la pondération de ces intérêts par rapport aux intérêts, libertés et droits fondamentaux des personnes concernées pèse en faveur du responsable du traitement (le « test de pondération »).*

En l'espèce, l'autorité de contrôle a considéré que si la finalité recherchée par l'agence pouvait être considérée comme légitime (à savoir « *afficher les qualités professionnelles et attirer l'attention de potentiels acquéreurs ou futurs vendeurs en leur permettant de se faire une idée plus précise sur le type de biens ayant déjà été commercialisé* »), les deux autres « tests » n'étaient pas remplis puisque la finalité recherchée pouvait être atteinte sans la publication des « *images avec les données d'identification* » de la personne et que le plaignant « *ne pouvait à aucun moment s'attendre à ce que les images de sa nouvelle maison soient publiées avec son adresse postale et/ou les numéros d'identification des parcelles cadastrales* ».

Compte tenu de ce qui précède, l'autorité de contrôle belge a ordonné à l'agence immobilière de se conformer à la demande d'exercice des droits de la personne, c'est-à-dire de procéder à l'effacement de l'adresse postale du bien immobilier et du numéro de parcelle cadastrale.

Source : ici

Un fournisseur d'électricité sanctionné pour le traitement de données inexactes

GDPD (Italie), 24 novembre 2022

L'autorité de contrôle italienne a sanctionné un fournisseur d'électricité pour avoir classé à tort un client comme « en retard de paiement » et ce, en raison de l'utilisation de données manifestement inexactes.

En Italie, lorsqu'un client souhaite changer de fournisseur d'électricité, le nouveau fournisseur sollicite les informations sur les arriérés de paiement auprès du fournisseur actuel. Si des arriérés existent, le nouveau fournisseur peut exercer son droit de rétractation et donc « refuser » le nouveau client.

En l'espèce, un client a déposé une plainte auprès de l'autorité de contrôle italienne lorsqu'il s'est rendu compte que son fournisseur d'électricité l'avait classé, à tort, comme « *client en retard de paiement* », ce qui a eu pour effet de l'empêcher de changer de fournisseur d'électricité.

Au cours de son enquête, l'autorité de contrôle a notamment constaté la violation du principe d'exactitude posé à l'article 5§1 d) du RGPD. Effectivement, en raison d'erreurs techniques sur le système informatique du fournisseur, de nombreuses informations erronées sur les arriérés de plusieurs clients étaient présentes dans le système. L'existence de données personnelles inexactes a eu pour conséquence d'engendrer près de 48.000 « *droits de rétractation* ».

En conséquence, l'autorité de contrôle italienne a infligé au fournisseur d'électricité une amende d'un million d'euros.

Source : ici

L'accès aux images de vidéosurveillance doit être restreint

ANSPDCP (Roumanie), 27 décembre 2022

L'autorité de contrôle roumaine a condamné un hypermarché pour n'avoir pas empêché un de ses salariés d'accéder aux images de vidéosurveillance.

Le salarié d'un hypermarché a pu accéder au local de vidéosurveillance et, à l'aide de son smartphone, a enregistré une vidéo sur laquelle apparaissait une personne avant de la publier sur internet.

La personne concernée, constatant l'existence d'une telle vidéo, s'est plainte auprès de l'hypermarché, qui a immédiatement notifié l'existence d'une violation de données à l'autorité de contrôle.

Dans ce contexte, l'autorité de contrôle a ouvert une enquête et a constaté que le responsable du traitement n'avait pas pris de mesures pour protéger les données et plus spécifiquement pour s'assurer que ses salariés n'aient pas accès aux images (art 29 du RGPD).

Compte tenu de ce qui précède, l'hypermarché a été condamné à une amende d'environ 3.000 €.

Source : ici

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 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 :