NEWSLETTER RGPD/DATA

NUMÉRO 53 ● 2023

SOMMAIRE

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

EN BREF

DROIT A REPARATION

- Le 4 mai 2023, la Cour de justice de l'Union européenne a été amenée à se prononcer sur les exigences requises en matière de droit à réparation résultant d'une violation du RGPD (plus d'infos ici)

CEPD

- Le 28 mars 2023, le Comité européen de la protection des données (CEPD) a mis à jour ses lignes directrices sur l'identification de l'autorité chef de file afin de clarifier les conditions de la désignation de l'autorité chef de file dans le cas spécifique de responsables conjoints de traitement. (plus d'infos ici)

- Le CEPD a adopté la version finale des lignes directrices sur le droit d'accès, le 28 mars dernier. Il délivre des orientations plus précises sur la mise en œuvre de ce droit. (plus d'infos ici)

- Le CEPD a mis à jour, le 28 mars 2023, ses lignes directrices initialement adoptées en 2017 sur les violations de données. (plus d'infos ici)

ACTUALITE

LA CNIL A DEBUTE SA CAMPAGNE DE CONTROLE DES DPO

Le 4 mai 2023, la CNIL a annoncé avoir débuté sa campagne de contrôle des DPO.

Dans sa communication du 15 mars 2023, le CEPD annonçait que le prochain « *CEF* » (cadre d'action coordonnée) porterait sur « *l'évaluation de la situation [des DPO]* », afin de vérifier le respect des règles relatives à la désignation, la fonction et aux missions du DPO.

Quelques jours plus tard, la CNIL confirmait que conformément au CEF, elle allait procéder « *à des vérifications sur la désignation et les modalités d'exercice des fonctions de DPO* ».

Ces vérifications ont débuté : dans une communication du 4 mai 2023, la CNIL a annoncé avoir adressé une douzaine de questionnaires à des établissements publics, des collectivités territoriales et des entreprises privées au cours du mois d'avril.

Une fois les questionnaires remplis par les organismes, les réponses seront analysées et pourront mener à des contrôles sur place afin de « *compléter les constatations* ».

Enfin, la CNIL annonce que d'éventuelles mesures correctrices pourront être émises telles que des mises en demeure ou des sanctions.

Dans ce contexte, les organismes sont invités à se questionner sur les conditions dans lesquelles leur DPO exerce ses missions et, le cas échéant, à se mettre en conformité.

Source : ici

DROIT AU DEREFERENCEMENT : DE NOUVELLES PRECISIONS DU CONSEIL D'ETAT

Par un arrêt du 20 avril dernier, le Conseil d'Etat, appliquant un récent arrêt de la CJUE, donne des éclairages sur les critères à prendre en compte cas de demande de déréférencement de liens renvoyant à des articles de presse relatant des condamnations pénales.

Pour rappel, le droit au déréférencement consiste pour une personne physique à obtenir de l'exploitant d'un moteur de recherche la suppression de liens/résultats associés à ses nom et prénom.

En l'espèce, une personne physique avait été condamnée pénalement, en première instance, notamment pour escroquerie, banqueroute, faux et usage de faux à 3 ans d'emprisonnement et à une interdiction de gérer une entreprise pendant 15 ans. Un journal avait publié un article concernant l'affaire sur son site internet, ledit article étant accessible via une recherche par le nom et prénom de la personne concernée sur le moteur de recherche Google (l'« Article »).

En appel, les peines avaient été réduites (2 ans d'emprisonnement et 10 ans d'interdiction de gérer une entreprise), mais aucun article n'avait été publié sur le sujet. Google ayant refusé de déréférencer l'Article à la demande de la personne concernée, cette dernière a porté plainte auprès de la CNIL, qui n'y a pas donné une suite favorable.

C'est dans ce contexte que le Conseil d'Etat a été saisie d'une demande d'annulation de la décision de la CNIL pour excès de pouvoir.

Dans sa décision, la Haute juridiction administrative a rappelé la position de la CJUE dans son arrêt du 24 septembre 2019 (affaire C-136/17), selon laquelle lorsque des liens accessibles depuis un moteur de recherche mènent vers des pages internet contenant des données personnelles relatives à des procédures pénales, l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données personnelles de la personne concernée est susceptible d'être particulièrement grave en raison de la sensibilité de ces données.

En conséquence, pour le Conseil d'Etat, la CNIL doit, « *en principe* », faire droit à une demande de mise en demeure du moteur de recherche concerné de déréférencer des liens vers des pages internet de site tiers (en l'occurrence, celui d'un journal) contenant ce type de données sensibles.

Le Conseil d'Etat a toutefois relevé une limite à cette règle de principe fondée sur le droit à la liberté d'information : si l'accès à l'information contenue sur ses pages internet, via une recherche à partir du nom de la personne concernée, *« est strictement nécessaire à l'information du public* », alors une telle demande de déréférencement n'a pas lieu d'être.

Pour pouvoir déterminer si une telle exception est applicable, la CNIL doit tenir compte de différents critères : (i) la nature des données en cause, leur contenu, leur caractère plus ou moins objectif, leur exactitude, leur source, les conditions et la date de leur mise en ligne et les répercussions que leur référencement est susceptible d'avoir pour la personne concernée, (ii) la notoriété de cette personne, son rôle dans la vie publique et sa fonction dans la société, (iii) et également la possibilité d'accéder aux mêmes informations à partir d'une recherche portant sur des mots-clés ne mentionnant pas le nom de la personne concernée.

Faisant application de ces critères, la Haute juridiction administrative a retenu que :

- L'Article, qui « *se rapporte à des faits antérieurs à 2014* », se borne à relater de façon générale la procédure concernant la personne concernée sans analyse ou commentaires « *de nature à nourrir un débat d'intérêt public* » ;
- La personne concernée, « *âgé*[e] *de 68 ans* », « *ne jouit pas d'une notoriété particulière* », l'affaire n'ayant pas fait l'objet « *d'autres commentaires publics* », la décision d'appel n'a pas fait non plus l'objet d'« *un article de presse référencé par le même moteur de recherche à partir de son nom* » ;
- L'Article « *n'est pas accessible en ligne à partir d'autres informations que le nom* [de la personne concernée] » ;
- L'Article ne reflète pas « *la situation judiciaire actuelle de* [la personne concernée] », compte tenu de la réduction de peine en appel.

En conséquence, selon le Conseil d'Etat « *eu égard aux répercussions que le référencement de cet article est susceptible d'avoir sur la situation personnelle de* [la personne concernée*], l'accès à ce contenu en ligne à partir du nom de* [cette dernière] *ne peut plus être regardé, à la date de la présente décision, comme strictement nécessaire à l'information du public* ». Il a donc jugé que la personne concernée est fondée à demander l'annulation de la décision de la CNIL et a enjoint celle-ci d'adresser une mise en demeure de déréférencement à GOOGLE.

Cette nouvelle jurisprudence permet de disposer d'éclairages précieux sur les critères dont doit tenir compte la CNIL, lorsqu'elle est amenée à se prononcer sur une demande de déréférencement de liens hypertextes renvoyant vers des pages de site internet de tiers, contenant des données personnelles relatives à des affaires pénales.

Source : ici

TRANSFERT DE DONNEES PERSONNELLES UE / ETATS-UNIS : UN CADRE TOUJOURS INSUFFISANT POUR LE PARLEMENT

Le 13 avril dernier, la commission des libertés civiles (« LIBE ») du Parlement européen a adopté un projet résolution concernant la décision d'adéquation des Etats-Unis. Celui-ci invite la Commission à ne pas adopter ce projet de résolution…

Si les députés européens soulignent que le cadre proposé est « *une amélioration* » par rapport « *aux cadres précédents* », cette amélioration n'est « *pas suffisante* ». A cet égard, les parlementaires ont, en particulier, souligné les insuffisances suivantes :

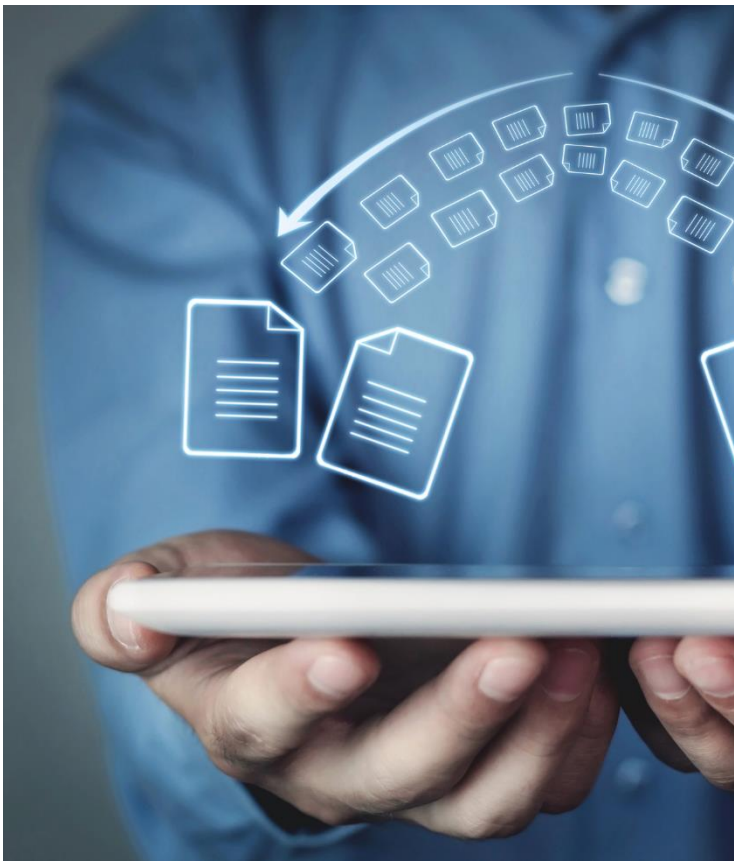
- Le fait qu'une collecte massive de données personnelles puisse être réalisée « *dans certains cas* », sans qu'elle soit soumise à « *une autorisation préalable indépendante* » ;
- L'absence « *de règles claires sur la conservation des données* » ;
- Le fait que la « *Cour de révision de protection des données* » qui serait créée, pour « *fournir réparation aux personnes concernées* », (i) prendrait des décisions « *secrètes, violant le droit des citoyens d'accéder aux données les concernant et de les rectifier* » ; et (ii) ne serait pas indépendante, dans la mesure où le Président des Etats-Unis pourrait révoquer ses juges et annuler ses décisions ;
- L'impossibilité actuelle d'analyser l' « *impact sur le terrain* » des « *pratiques sur la base du cadre de confidentialité des données* » de la communauté américaine de renseignement, compte tenu qu'elle les « *met toujours à jour* » ;

Les parlementaires craignent, par ailleurs, une nouvelle invalidation du cadre proposé par le CJUE et invitent ainsi la Commission européenne à « *veiller à ce que le futur cadre puisse résister aux défis juridiques et apporter une sécurité juridique aux citoyens et aux entreprises de l'UE* ».

En conclusion, ils invitent la Commission à ne pas valider la décision d'adéquation proposée et de rouvrir les négociations avec les Américains sur ce cadre de transfert de données.

A suivre…

Source : ici



LE RAPPORT D'ACTIVITE DU CEPD POUR 2022

Le Comité européen pour la protection des données personnelles (CEPD) a publié, le 17 avril 2023, son rapport d'activité retraçant les actions réalisées au cours de l'année 2022.

Après avoir récemment publié son programme de travail pour 2023-2024, le CEPD revient sur l'année 2022 dans son rapport d'activité, publié le 17 avril 2023.

En introduction, la présidente du CEPD se félicite de l'impact qu'a eu le RGPD, qui est au cœur de la législation récemment adoptée concernant le marché unique numérique, et de la prise de conscience des organisations présentes au-delà des frontières de l'UE, qui sont aujourd'hui conscientes qu'elles ne peuvent conduire leurs affaires en Europe sans se conformer au RGPD.

La présidente considère que le CEPD est un acteur majeur dans l'économie numérique de l'EEE et qu'il ne s'assure pas simplement de l'application du RGPD, mais aide également l'Europe à forger son « *futur numérique* ».

Dans son rapport d'activité, le CEPD met en exergue l'assistance fournie par son secrétariat aux différentes autorités de contrôle. A titre d'exemple, le CEPD indique que son secrétariat fournit des solutions informatiques facilitant la communication entre autorités.

Outre l'inventaire des lignes directrices et décisions contraignantes qu'il a émises au cours de l'année 2022, le CEPD évoque les décisions marquantes prises par les autorités de contrôle nationales.

Source : ici

L'UTILISATION DU FICHIER SIRENE PAR LES DOUANES EST ILLICITE

Constatant l'utilisation illicite d'un fichier recensant des informations sur les passagers des navires contrôlés, la CNIL a mis en demeure le Ministère de l'Economie, auquel les douanes sont rattachées, de se mettre en conformité.

La CNIL a reçu un signalement faisant état de l'utilisation, par un service des douanes, du fichier « SIRENE » (*Système d'Information du REnseignement des Navires et Equipages* »).

Les douanes utilisaient ce fichier SIRENE, (à ne pas confondre avec le répertoire SIRENE qui recense les entreprises françaises) afin de recenser, de manière quasi systématique, tous les individus contrôlés en mer ou à quai. Ce fichier contenait les données de 45 793 personnes (dont 392 mineurs).

Au cours de son enquête, la CNIL a constaté de nombreux manquements :

- **Manquement relatif à la licéité du traitement et à l'absence d'analyse d'impact**

La CNIL a d'abord relevé que le fichier SIRENE poursuivait une finalité de prévention, détection et d'enquête dans le cadre d'infractions pénales, or, les traitements mis en œuvre pour le compte de l'Etat pour une telle finalité doivent être prévus par une disposition législative ou réglementaire soumis à l'avis de la CNIL, ce qui n'était pas le cas en l'espèce.

De même, le traitement était, selon la CNIL, susceptible d'engendrer un risque élevé pour les droits et libertés des personnes en raison (i) du nombre de personnes concernées et surtout (ii) « *d'un traitement de données de localisation à large échelle* », et aurait donc dû faire l'objet d'une analyse d'impact adressée à la CNIL.

- **Manquement à la distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées**

La CNIL a ensuite relevé que le fichier n'opérait pas de distinction entre les catégories de personnes recensées, autrement dit qu'il n'y avait pas de distinction entre (i) les personnes soupçonnées d'une infraction, (ii) les coupables, (iii) les victimes et (iv) les tiers. Or, la loi Informatique et Libertés fait obligation, en cas de traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'opérer « *une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées* ». Cette absence de distinction entre les catégories de personnes constituait, selon la CNIL, un manquement à la loi Informatique et Libertés.

- **Manquement relatif à l'information des personnes**

La CNIL a enfin constaté que lorsque des navires étaient contrôlés, les personnes présentes faisaient régulièrement l'objet d'un fichage dans le fichier SIRENE (i) sans qu'elles connaissent l'existence dudit fichier, et, par conséquent, (ii) sans les informer. Cette absence d'information est contraire à la loi Informatique et Libertés.

Compte tenu de ces manquements, la CNIL a mis en demeure le Ministère de l'Economie de remédier aux manquements précédemment exposés dans un délai de six mois ou, « à *défaut, de cesser de procéder au traitement des données* ».

Source : ici

DOCTRINE

RGPD

Réutilisation de données et changement de finalité : test de compatibilité

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 problématique de l'exploitation par le responsable du traitement d'images obtenues grâce à un dispositif de vidéosurveillance, mais pour une finalité différente que celle initialement prévue.

Il ressort des termes de l'article 5 du RGPD que les données sont notamment collectées et traitées, d'une part, de manière loyale et licite et, d'autre part, « *pour des finalités déterminées, explicites et légitimes* ». Le texte ajoute que ces données ne peuvent être traitées « *ultérieurement de manière incompatible avec ces finalités* ». En d'autres termes, le responsable du traitement ne peut, en principe, exploiter les données qu'il a initialement collectées que pour la finalité pour laquelle il a opéré la collecte desdites données. Il ne peut donc utiliser les données pour un autre but que celui qui a été fixé. Ainsi, un fichier de recrutement de candidats pour une offre d'embauche ne peut pas être utilisé pour proposer à ces candidats des offres commerciales.

Toutefois, et comme l'indique l'article 5 susvisé, ce principe de limitation doit être nuancé, lorsque la finalité ultérieure est compatible avec la finalité initiale, ce que confirme le considérant 50 du RGPD : « *le traitement de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement ne devrait être autorisé que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement* ».

Il appartient donc au responsable du traitement qui souhaite réutiliser les données collectées pour une autre finalité, de réaliser un test de compatibilité. Pour ce faire, il doit notamment tenir compte: (i) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données personnelles ont été collectées et les finalités du traitement ultérieur envisagé ; (ii) du contexte dans lequel les données personnelles ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ; (iii) de la nature des données personnelles, en particulier si le traitement porte sur des données sensibles ou des données personnelles relatives à des condamnations pénales et à des infractions ; (iv) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ; (v) de l'existence de garanties appropriées.

L'affaire[1]

Un particulier avait été signalé pour avoir enfreint les règles de confinement mises en œuvre pour lutter contre la propagation du COVID-19. Ce signalement avait été réalisé grâce aux images issues du dispositif de vidéosurveillance installé dans les rues de la municipalité de Salento.

Considérant que ce traitement était contraire à la règlementation sur la protection des données personnelles, le particulier a déposé une plainte auprès de l'autorité de contrôle italienne (la « *GPDP* »). Rappelant que si une municipalité est en droit, en application des textes, d'utiliser un dispositif de vidéosurveillance installé sur la voie publique « *à des fins de sécurité urbaine* », ce dispositif ne peut être exploité pour un autre objectif, en application du principe de limitation des finalités. Or, en l'espèce, la municipalité avait traité les images litigieuses dans un but qui n'était pas la sécurité publique, mais la répression des comportements contraires aux mesures d'endiguement de la pandémie.

La question se posait alors de la compatibilité des deux finalités, étant précisé qu'il ne peut y avoir, en principe, une relation entre la finalité initiale et la finalité du traitement ultérieur que si ce dernier est déjà, dans une certaine mesure, « *implicite* » ou peut être considéré comme une « *suite logique* » du traitement initial. La GPDP a considéré que ce n'était pas le cas en l'espèce, expliquant que le traitement visant à constater une infraction aux règles de confinement « *ne peut en aucun cas être considéré comme logiquement lié ou dérivant du traitement mis en place par la municipalité aux fins de sécurité urbaine, qui vise à prévenir et combattre les phénomènes de criminalité généralisée* ».

Par ailleurs, l'autorité de protection des données a souligné que : « *le recours à la vidéosurveillance sur la voie publique en tant que mesure visant à contenir la pandémie (...) est également contraire aux attentes des citoyens concernant le traitement de leurs données, qui, compte tenu également des dispositions du règlement municipal sur la vidéosurveillance adopté par la municipalité, étaient convaincus que les images capturées par les caméras installées sur la voie publique seraient traitées exclusivement aux fins de la sécurité urbaine susmentionnée* ».

Enfin, la GPDP a relevé que la municipalité n'avait adopté aucune « *garantie spécifique* » afin de réduire l'impact du traitement sur les citoyens et d'assurer la loyauté dudit traitement, dès lors qu'elle n'a fourni aux personnes concernées « *aucune information spécifique sur la finalité du traitement poursuivie* » à savoir la détection des violations administratives des règles d'urgence pour le confinement.

Dans ces conditions, le traitement des images litigieuses par la municipalité a été considéré comme illicite car réalisé en violation notamment des dispositions de l'article 5 du RGPD.

Quelles recommandations ?

La première recommandation serait d'identifier, pour un traitement donné, toutes les finalités « *légitimes* » dudit traitement afin d'étendre son périmètre, sous réserve (i) que ces finalités soient « *déterminées, explicites* » et (ii) que les données soient traitées de manière « *loyale et transparente* ». La seconde recommandation serait, dans le cas où le responsable du traitement souhaiterait traiter les données pour une finalité différente de la ou des finalité(s) initialement prévue(s), de réaliser un test de compatibilité. Cet exercice est fondamental car, en cas d'incompatibilité, le nouveau traitement serait considéré comme illicite et les éléments de preuve obtenus au moyen dudit traitement (par exemple : un dispositif de vidéosurveillance) pourraient être considérés, devant une juridiction civile, comme déloyaux et donc inopposables à la personne concernée.

Alexandre FIEVEE
Avocat associé
DERRIENNIC Associés

Notes

(1) GPDP, ordonnance d'injonction, 20 octobre 2022.

PANORAMA EUROPÉEN

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

Clôture obligatoire de la messagerie électronique d'un collaborateur en cas de départ

GDPD (Italie), 11 janvier 2023

Une société a été sanctionnée par l'Autorité de contrôle italienne pour avoir accédé à la messagerie électronique d'un ancien collaborateur et transféré les courriels reçus par celui-ci vers un autre compte de messagerie.

A la suite de son départ d'une société, un ancien collaborateur a constaté que son adresse de messagerie électronique était toujours active. Il a donc exercé son droit à l'effacement en sollicitant « *la désactivation de l'adresse électronique* ».

La société n'a pas immédiatement fait droit à sa demande en considérant que le maintien du compte de messagerie (i) était nécessaire à l'exercice de son droit en justice (le collaborateur ayant saisi la justice italienne après son départ), et (ii) avait pour finalité de ne « *pas interrompre brusquement le contact avec les clients* ».

L'ancien collaborateur a déposé une plainte devant l'Autorité de contrôle italienne qui a constaté, au cours de son enquête, plusieurs manquements au RGPD, la société ayant :

- utilisé l'adresse électronique du collaborateur pour « *envoyer un courriel à certains contacts* » afin d'indiquer que le collaborateur ne faisait plus partie de la société.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Selon l'Autorité, un tel traitement est contraire au principe de minimisation dès lors que le responsable du traitement pouvait mettre en œuvre « *un traitement moins invasif* » pour poursuivre les finalités de maintien des relations clients ;

- « *consulté la correspondance envoyée et reçue* [par le collaborateur] *pendant la collaboration* » et « *mis en place un système automatique de transfert des courriels reçus après le départ de la société, vers une autre personne* ».

Selon l'Autorité, un tel traitement est contraire au principe de minimisation pour les mêmes raisons que celles précédemment évoquées et est dépourvu de base légale notamment car certaines correspondances produites en justice étaient des correspondances privées.

- omis d'informer le collaborateur sur l'existence de tels traitements, en contradiction avec l'article 12 du RGPD ;
- empêché le collaborateur d'exercer ses droits et ne répondant pas de manière adéquate à la demande d'effacement, en contradiction avec l'article 17 du RGPD.

En conséquence, l'Autorité de contrôle a prononcé une amende de 5.000 € à l'encontre de la société.

Source : ici

Régime de la séparation des biens : traiter les données personnelles de l'autre époux est illicite

CTPD (Andalousie), 2023

L'Autorité de contrôle andalouse a sanctionné une municipalité pour avoir traité les données personnelles d'un homme afin de lui saisir sa pension au titre de dettes contractées par sa femme alors que le couple était marié sous le régime de la séparation des biens.

Une municipalité a transmis à une personne un « *avis de saisie de sa pension* » afin de recouvrer les dettes contractées par son épouse.

Considérant qu'étants mariés sous le régime de la séparation des biens il n'était pas débiteur solidaire et n'avait donc pas à recevoir un tel avis de saisie, le mari a déposé une plainte devant de l'Autorité de contrôle andalouse.

Il reprochait à la municipalité de multiples manquements au RGPD, dès lors que cette dernière (i) a traité ses données personnelles sans base légale, (ii) a demandé illégalement à une autre administration des données personnelles le concernant, et (iii) n'aurait pas dû lui transmettre les données personnelles de son épouse.

Au cours de son enquête, l'Autorité de contrôle a constaté que la municipalité avait « *présumé le régime de la communauté de biens* », la poussant à « *considérer à tort le mari comme faisant partie de la procédure de recouvrement de la dette contractée […] par son épouse* ».

En se basant sur cette présomption erronée, la municipalité avait sollicité d'une administration tierce les informations personnelles du mari afin de lui transmettre l'avis de saisie.

Rappelant les règles applicables au titre du RGPD, l'Autorité de contrôle a considéré que la municipalité « *aurait dû effectuer les démarches et les consultations nécessaires pour vérifier si les époux étaient mariés sous le régime de la communauté des biens* ». Cette vérification aurait permis, selon l'Autorité, d'éviter (i) « *la communication de données personnelles sans base légale* », et (ii) « *l'ouverture d'une procédure de saisie de la pension* » du mari.

Plus précisément, l'Autorité de contrôle a estimé (i) qu'en consultant une autre administration afin de recevoir les données personnelles d'un individu et (ii) en communiquant à ce dernier les données à caractère personnel de sa femme dans l'avis de saisie, la municipalité a traité des données personnelles sans base légale, enfreignant ainsi l'article 6 du RGPD.

En conséquence, l'Autorité de contrôle a prononcé un rappel à l'ordre à l'encontre de la municipalité.

Source : ici

Violation de données : la notion de « courte période d'enquête »

Datatilsynet (Norvège), 8 mars 2023

L'Autorité de contrôle norvégienne a sanctionné un responsable du traitement pour avoir attendu 3 mois entre la prise de connaissance de l'impact de l'incident sur des données personnelles et la notification de cet incident.

Une entreprise américaine spécialisée dans la conception et le développement de dispositifs médicaux a subi un incident de sécurité : un tiers non identifié a accédé, de manière non autorisée, au compte de messagerie électronique du vice-président des ressources humaines et a ainsi eu accès à de nombreuses données personnelles financières de salariés (salaires, avantages...). L'équipe de sécurité informatique, alertée le 14 juin 2021, a immédiatement mis en œuvre des mesures de sécurité pour endiguer l'incident et comprendre l'origine de la faille.

Le 19 juillet 2021, l'enquête interne de l'entreprise a permis de découvrir que les données personnelles des employés européens avaient été affectées par l'incident : l'entreprise ne l'a pas immédiatement notifié à l'Autorité de contrôle, mais a procédé à une évaluation préalable afin de déterminer si l'incident devait être notifié à l'Autorité de contrôle et, le cas échéant, aux personnes concernées.

Le 24 septembre 2021, l'entreprise a finalement notifié à l'Autorité de contrôle norvégienne une violation de données personnelles, conformément à l'article 33 du RGPD.

A la suite de cette notification, l'Autorité de contrôle norvégienne a ouvert une enquête et a constaté que l'entreprise avait attendu 67 jours entre le moment où elle a pris « *connaissance* [du fait] *que l'incident affectait les données personnelles de personnes dans l'UE* » (19 juillet) et la notification (24 septembre).

Rappelant l'obligation pour le responsable du traitement de notifier une violation de données à caractère personnel à l'Autorité de contrôle compétente « *dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance* », l'Autorité de contrôle a considéré que l'entreprise avait violé cette obligation.

En effet, selon l'Autorité de contrôle, « *étant donné que le 19 juillet 2021, [le responsable du traitement] disposait d'éléments suffisants pour conclure, avec un degré raisonnable de certitude, qu'une violation de données à caractère personnel avait eu lieu, [le responsable du traitement] aurait pu et dû soumettre une notification initiale " sans retard injustifié " à partir de cette date* ».

Compte tenu de ce qui précède, l'Autorité de contrôle a infligé au responsable du traitement une amende d'environ 210 000 euros pour avoir manqué à l'obligation prévue par l'article 33 du RGPD de notifier toute violation des données personnelles dans les meilleurs délais. Ce montant élevé s'explique en partie par « *la manière dont l'infraction a été portée à la connaissance* » de l'Autorité de contrôle, puisqu'il était reproché au responsable du traitement d'avoir laissé croire qu'il n'avait eu connaissance d'une violation de données à caractère personnel que le 21 septembre.

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 2023 :
Sur demande.
Lieu de la formation :
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 P
Inscription et informations :