NEWSLETTER RGPD/DATA

NUMÉRO 52 ● 2023

SOMMAIRE

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

REQUETE « 145 » : LE DROIT A LA PROTECTION DES DONNEES N'EST PAS ABSOLU

La Cour de cassation a rendu une décision admettant qu'une salariée puisse demande communication, sur le fondement de l'article 145 du Code de procédure civile, des bulletins de salaire de ses collègues masculins, aux fins de preuve dans le cadre d'une action en discrimination.

Une salariée licenciée a considéré avoir subi une inégalité salariale par rapport à certains collègues masculins ayant occupé le même poste qu'elle.

Dans ce contexte, cette salariée a saisi la formation de référé de la juridiction prud'homale, afin d'obtenir la communication d'éléments de comparaison détenus par ses deux employeurs successifs, sur le fondement de l'article 145 du Code de procédure civile.

La salariée a obtenu gain de cause, la Cour d'appel de Paris ordonnant aux deux sociétés concernées la communication, à la salariée, « *sur une période comprise entre 2013 et 2019, [des] bulletins de paie de huit autres salariés, laissant apparaître leurs noms et prénoms, leurs classifications conventionnelles, leurs rémunérations mensuelles détaillées (fixes et variables) et leurs rémunérations brutes totales cumulées par année civile* ».

Les deux sociétés concernées ont formé un pourvoi devant la Cour de cassation, alléguant que cette communication était contraire aux exigences du RGPD, notamment en raison de son incompatibilité avec la finalité initiale pour lesquelles ces données avaient été collectées. Le juge ayant ordonné cette communication n'avait, par ailleurs édicté aucune garantie en matière de sécurité, de confidentialité et de limitation de la durée de conservation.

Enfin, selon les requérantes, le droit à la preuve ne peut pas justifier la production d'éléments portant atteinte à la vie privée, sauf si cette production est indispensable à l'exercice d'un droit et si l'atteinte à la vie privée est proportionnée au but poursuivi. Pour les requérantes, cela n'était pas le cas, la salariée étant déjà en mesure de présenter des éléments susceptibles de laisser présumer de l'existence de la discrimination alléguée.

La Cour de cassation a, dans une décision du 8 mars 2023, rejeté le pourvoi au motif le droit à la protection des données personnelles n'est pas absolu et qu'il appartient au juge saisi de la requête de 145 d'évaluer la nécessité et la proportionnalité de la communication. En l'occurrence, la Cour d'appel de Paris a estimé que la salariée était bien fondée à obtenir les bulletins de salaire afin de présenter des éléments laissant présumer l'existence de l'inégalité salariale et que la communication était indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, à savoir « *la défense de l'intérêt légitime de la salariée à l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail* ».

Source : ici

DECISION D'ADEQUATION CONCERNANT LES ETATS-UNIS : LES RETICENCES DU PARLEMENT EUROPEEN

Le Parlement européen a adopté une résolution au sujet du projet de décision d'adéquation concernant les transferts de données personnelles vers les Etats-Unis. Pour le Parlement, les garanties avancées par les Etats-Unis sont largement insuffisantes.

Pour rappel, la Cour de justice de l'Union européenne a, dans une décision « Schrems II » du 16 juillet 2020, invalidé le Privacy Shield et a fortement restreint les possibilités de transfert de données personnelles vers les Etats-Unis. Cette décision était motivée par les lois et pratiques américaines, lesquelles permettent des accès par les autorités de surveillance américaines aux données personnelles jugés trop larges.

Suite à la signature d'un décret présidentiel par les Etats-Unis, visant à renforcer les garanties portant sur les activités de renseignement des Etats-Unis, notamment en les soumettant à des exigences de proportionnalité et de nécessité, la Commission européenne a, le 13 décembre 2022, amorcé le processus tendant à l'adoption d'une décision d'adéquation concernant les transferts de données entre l'Union européenne et les Etats-Unis.

Dans ce cadre, la Commission a soumis son projet de décision d'adéquation au Parlement européen, qui dispose d'un droit de regard.

Le 14 février 2023, le Parlement européen a adopté une résolution portant sur le projet de décision de la Commission européenne, qui se révèle très critique à l'égard des positions prises par la Commission. Il y est notamment indiqué que :

- les Etats-Unis ne disposent pas de loi fédérale, applicable à l'ensemble du pays, concernant la vie privée et la protection des données personnelles, au contraire de l'intégralité des autres pays du Monde ayant bénéficié d'une décision d'adéquation ;
- les notions de « *nécessité* » et de « *proportionnalité* », mentionnées par le décret présidentiel américain, font l'objet de définitions différentes de part et d'autre de l'Atlantique, et seront ici interprétées uniquement à la lumière de la loi américaine ;
- le décret présidentiel américain ne prohibe pas la collecte massive de données ;
- la liste des « *objectifs de sécurité nationale légitimes* », justifiant la collecte de données personnelles, peut être étendue par le Président des Etats-Unis, qui peut choisir de ne pas révéler cette extension au public ;
- le décret présidentiel américain ne s'applique pas aux accès aux données collectées par des autorités publiques par le biais du Cloud Act ou du Patriot Act, ni aux moyen d'opérations d'achat ou de partage de données.

Par ailleurs, de façon générale, pour le Parlement européen, le décret présidentiel américain n'est ni clair, ni précis, ni prévisible quant à son application.

Le Parlement européen met également en exergue les limites du mécanisme de recours ouvert aux citoyens européens, devant la « *Data Protection Review Court* » (« *DPRC* »), en relevant que :

- les décisions de la DPRC seront classifiées et inaccessibles au public ou au plaignant ;
- la DPRC est rattachée au pouvoir exécutif, et non au pouvoir judiciaire ;
- le plaignant sera représentée par un « *special advocate* » désigné par la DPRC elle-même, pour lequel il n'existe aucune exigence d'indépendance ;
- les décisions de la DPRC ne peuvent octroyer de dommages et intérêts au plaignant et ne peuvent pas faire l'objet d'appel devant une cour fédérale.

En raison de ces différents éléments, le Parlement européen a estimé que la DPRC ne remplit pas les conditions d'indépendance et d'impartialité de l'article 47 de la Charte des droits fondamentaux de l'UE.

La conclusion globale du Parlement européen est que le projet de décision d'adéquation de la Commission européenne ne permet pas d'assurer une équivalence en matière de protection des données personnelles. Le Parlement demande donc à la Commission de ne pas adopter le projet de décision et de continuer ses négociations avec ses interlocuteurs américains afin de créer un mécanisme aboutissant à une telle équivalence.

Source : ici

DECISION D'ADEQUATION CONCERNANT LES ETATS-UNIS : L'AVIS DU CEPD

Le 28 février 2023, le CEPD a rendu son avis sur le projet de décision d'adéquation de la Commission européenne concernant les Etats-Unis.

Pour rappel, la Cour de justice de l'Union européenne a, dans une décision « Schrems II » du 16 juillet 2020, invalidé le Privacy Shield et a fortement restreint les possibilités de transfert de données personnelles vers les Etats-Unis. Cette décision était motivée par les lois et pratiques américaines, lesquelles permettent des accès par les autorités de surveillance américaines aux données personnelles jugés trop larges.

Suite à la signature d'un décret présidentiel 14086 par les Etats-Unis, visant à renforcer les garanties portant sur les activités de renseignements des Etats-Unis, notamment en les soumettant à des exigences de proportionnalité et de nécessité, la Commission européenne a, le 13 décembre 2022, amorcé le processus tendant à l'adoption d'une décision d'adéquation concernant les transferts de données entre l'Union européenne et les Etats-Unis.

Le 28 février 2023, le CEPD a rendu son avis quant au projet de décision d'adéquation de la Commission.

Le CEPD y salue les améliorations substantielles, telle que l'introduction d'exigences incorporant les principes de nécessité et de proportionnalité pour la collecte de données par les services de renseignements américains.

Le CEPD y exprime également ses préoccupations et demande des éclaircissements sur plusieurs points, notamment :

- **Les droits des personnes concernées**, le CEPD déplorant les éléments suivants :
    - Le droit d'accès n'est pas décrit dans le corps de la décision d'adéquation.
    - L'exercice du droit d'opposition semble, quant à lui, cantonné au cas de figure où les données sont utilisées à des fins de prospection directe.
- **Les transferts ultérieurs**, qui ne doivent pas amoindrir le niveau de protection des personnes concernées. Le CEPD recommande, à ce titre, que les destinataires ultérieurs des données soient soumis à des règles, y compris contractuel, permettant un niveau de protection adéquate.
- **Le champ d'application des exemptions**, jugé peu clair par le CEPD, la décision d'adéquation prévoyant que l'adhésion aux principes qu'elle liste puisse être limitée, notamment afin que le destinataire des données se conforme à la loi, à des exigences de sécurité nationale, à une décision de justice ou à la poursuite d'intérêts publics. Le CEPD n'ayant pas connaissance des lois américaines, il n'est pas en mesure d'évaluer le détail du champ de ces exemptions, et demande donc à la Commission de préciser ces cas d'exemption.

- **Les collectes de données indiscriminées à large échelle**, qui demeurent toujours possible, à condition d'être temporaires, et ce sans nécessiter de garantie, telle qu'une autorisation. Le CEPD demande à la Commission d'encadrer précisément ces cas de collecte.

- **Le fonctionnement pratique du mécanisme de recours**, jugé, par le CEPD, identique à celui figurant dans la décision Privacy Shield, au sujet duquel le CEPD avait déjà émis des critiques.

Le CEPD apprécierait, enfin, que l'entrée en vigueur et l'adoption de la décision d'adéquation soient subordonnées à l'adoption, par toutes les agences de renseignement américaines, de politiques et de procédures actualisées visant à mettre en œuvre le décret présidentiel 14086.

Source : ici

LES THEMATIQUES DE CONTROLES DE LA CNIL POUR 2023

Comme chaque année, la CNIL a publié ses « thématiques prioritaires », qui orientent sa politique de contrôle sur des sujets à fort enjeu pour le public et permettent d'évaluer la conformité de secteurs ciblés.

Dans une publication du 15 mars 2023, la CNIL a partagé ses thématiques de contrôle prioritaires pour l'année 2023.

Ces thématiques sont les suivantes :

- **L'utilisation de caméras « *augmentées* »**, par les acteurs publics, notamment par les collectivités territoriales, dans le cadre des manifestations sportives de grande ampleurs prévues en 2023, telles que les Jeux olympiques et la Coupe du monde de rugby.

- **L'utilisation du fichier des incidents de remboursement de crédits aux particuliers**, qui est géré par la Banque de France et recense les informations sur les incidents de paiement caractérisés liés aux découverts et aux crédits accordés pour des besoins non professionnels.

  La CNIL indique que ce fichier représente un enjeu particulièrement fort, puisque les données qui y sont contenues peuvent conditionner l'octroi de crédit. Elle contrôlera donc les conditions dans lesquelles les banques accèdent à ce fichier, en extraient des informations et les tiennent à jour après régularisation des incidents de paiement.

- **L'accès au dossier patient informatisé (« DPI ») au sein des établissements de santé**. La CNIL indique que la sécurité des données de santé, qui avait déjà été retenue comme thématique annuelle des contrôles en 2020 et en 2021, demeure une question récurrente dans un grand nombre de dossiers qui lui sont soumis et concerne l'ensemble des établissements de santé.

  La CNIL fait, à ce titre, état de nombreuses plaintes reçues dénonçant les accès, par des tiers non autorisés, au DPI au sein d'établissements de santé.

- **Le traçage des utilisateurs par les applications mobiles**. La CNIL a relevé que les fabricants de téléphones mettent à disposition des éditeurs d'applications des identifiants permettant un suivi des utilisateurs pour des objectifs publicitaires, statistiques ou techniques. La CNIL assimile l'usage de ces identifiants à celle des cookies et relève que ces identifiants sont utilisés sans information ni consentement des utilisateurs.

Enfin, la CNIL annonce qu'elle va procéder à des vérifications sur la désignation et les modalités d'exercice des fonctions du délégué à la protection des données (DPO).

Source : ici

LE PROGRAMME DE TRAVAIL DU CEPD POUR 2023-2024

Dans un document adopté le 14 février 2023 et publié le 22 février sur son site internet, le CEPD a partagé son programme de travail pour les années 2023 et 2024.

Le CEPD a rédigé son programme pour les années 2023 et 2024, sous forme de « *piliers* », reflets de la stratégie du CEPD et des besoins prioritaires identifiés par ses membres.

Le premier pilier consiste à améliorer l'harmonisation et faciliter la conformité. Il s'agit, pour le CEPD, de développer et promouvoir des outils facilitant la mise en œuvre concrète de la protection des données, en prenant en compte les expériences pratiques des différents membres du CEPD. Dans ce contexte, le CEPD annonce travailler sur des lignes directrices concernant plusieurs sujets, tels que : l'intérêt légitime, le traitement de données d'enfants, ou encore le traitement de données à des fins médicales et de recherches scientifiques.

Le deuxième pilier consiste à contribuer à l'implémentation pratique d'une coopération efficace entre les autorités de contrôle. Le CEPD entend fluidifier les procédures internes, combiner les expertises et promouvoir la coordination améliorée, et annonce travailler sur des lignes directrices en matière d'assistance mutuelle, ainsi que sur un modèle de plainte pour les personnes concernées.

Le troisième pilier consiste à aborder les nouvelles technologies sous le prisme des droits fondamentaux.

A ce titre, le CEPD surveillera les technologies nouvelles et émergentes, ainsi que leurs impacts sur les droits fondamentaux et la vie quotidienne des personnes. A ce titre, le CEPD travaille sur des lignes directrices en matière d'anonymisation, de pseudonymisation et de blockchain, ainsi qu'en matière d'interconnexion entre l'IA Act et le RGPD.

Enfin, selon le quatrième pilier, intitulé « *La dimension mondiale* », le CEPD assurera la promotion des standards de protection des données européens, dans le cadre des transferts de données vers des pays tiers à l'UE, et, de façon plus générale, la promotion de ces standards comme modèle mondial afin d'assurer la protection des données personnelles au-delà des frontières de l'UE.

Source : ici

LE DPO DANS LE VISEUR DU CEPD

Le CEPD a annoncé que le thème de son « cadre d'action coordonné » 2023 était « la désignation et la position des DPO ».

Créé en 2020, le « *cadre d'action coordonné* » (CEF en anglais) vise à « *faciliter [entre les autorités de contrôle] des actions conjointes […], allant de la sensibilisation et la collecte d'informations conjointes à des opérations répressives ciblées et coordonnées et des enquêtes conjointes* ».

Dans une communication du 15 mars 2023, le CEPD a annoncé que le prochain CEF porterait sur « *l'évaluation de la situation [des DPO*] » afin de vérifier que ces derniers « *occupent au sein de leur organisation la position requise par les articles 37 à 39 du RGPD* », c'est-à-dire vérifier le respect des règles relatives à la désignation, la fonction et les missions du DPO.

A cette fin, les DPO recevront des questionnaires afin de remonter des problèmes et/ou difficultés et les autorités de contrôle pourront ouvrir des enquêtes afin d'analyser la situation des DPO.

Dans son article annonçant les « *thématiques prioritaires de contrôle 2023* » la CNIL a d'ailleurs confirmé qu'en vertu de ce CEF, elle allait procéder à des « *vérification sur la désignation et les modalités d'exercice des fonctions de DPO* ».

Source : ici

VU DANS LA PRESSE

« DSIH », AVRIL 2023

RECHERCHES MEDICALES : RAPPEL A L'ORDRE DE LA CNIL

La présidente de la CNIL a rappelé à deux organismes procédant à des recherches médicales leurs obligations légales.

Deux organismes procédant à des recherches médicales entre janvier et juillet 2022 ont fait l'objet d'un signalement ayant donné lieu à un contrôle de la CNIL. Cette dernière a constaté plusieurs manquements aux règles sur la protection des données, dont l'absence d'analyse d'impact et la délivrance aux patients concernés d'une information incomplète[1].

1. *Sur l'obligation de réaliser une étude d'impact*

A titre liminaire, la CNIL a rappelé qu' « à l'exception des recherches internes (réalisées à partir des données collectées pendant les soins par les professionnels de santé prenant en charge les patients, et pour leur usage exclusif), les recherches en santé doivent être autorisées par la CNIL ou être conformes à une méthodologie de référence*. »*

Ces méthodologies sont au nombre de six dont :

- Pour les recherches impliquant la personne humaine :
    - La MR-001, pour les recherches interventionnelles et les recherches interventionnelles à risques et contraintes minimes ;
    - La MR-002 ou la MR-003, pour les recherches non-interventionnelles ;
- Pour les recherches n'impliquant pas la personne humaine, la MR-004.

En application de ces méthodologies, une analyse d'impact doit être réalisée et ce, avant le démarrage de la recherche.

A titre d'illustration, la méthodologie de référence « MR-001 » indique que : « *Le responsable du traitement doit effectuer une analyse d'impact relative à la protection des données, qui doit couvrir en particulier les risques sur les droits et libertés des personnes concernées. Il met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques identifiés. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires.* »

Ce n'est qu'une fois l'analyse d'impact réalisée que le responsable du traitement est censé être en mesure de décider entre :

- Une demande d'autorisation à la CNIL (hypothèse dans laquelle l'analyse d'impact révèle que les traitements envisagés dans le cadre de la recherche ne sont pas conformes à la méthodologie de référence applicable) ; ou
- Un engagement de conformité à la méthodologie de référence applicable (hypothèse dans laquelle l'analyse d'impact révèle que les traitements envisagés dans le cadre de la recherche sont conformes à la méthodologie de référence applicable).

En l'espèce, les deux organismes visés par le contrôle de la CNIL n'avaient réalisé aucune analyse d'impact concernant les recherches médicales menées.

2. Sur l'obligation d'informer les personnes concernées

La CNIL a constaté que l'information délivrée par les deux organismes aux personnes participant aux recherches était incomplète. L'autorité de contrôle a notamment souligné que « *les feuillets d'information remis par les deux organismes ne précisaient ni la nature des informations collectées ni leur durée de conservation* ». Par ailleurs, ces supports n'indiquaient pas les coordonnées du délégué à la protection des données, ni les modalités de recours auprès de la CNIL.

Enfin, et surtout, la CNIL a relevé qu'une notice d'information affirmait que les données étaient anonymisées, ce qui n'était pas le cas, « *puisque l'identité des patients était seulement remplacée par un "numéro patient" à trois chiffres et un "code patient" composé de deux lettres correspondant à la première initiale du nom et du prénom de la personne concernée* ».

Ainsi, et comme l'a souligné la CNIL : « *Cette procédure aboutit à une pseudonymisation des données, et non à une anonymisation, dans la mesure où il demeurait possible d'isoler un individu dans le jeu de données et de le réidentifier.* »

Il convient de relever, sur ce dernier point, que les méthodologies des référence susvisées n'imposent pas aux organismes une anonymisation des données de santé, mais une simple pseudonymisation. Elles prévoient d'ailleurs un régime distinct selon que les données sont « *directement identifiantes* » ou « *indirectement identifiantes* » (et donc pseudonymisées). Ainsi, seules ces dernières peuvent être communiquées au responsable du traitement (à savoir l'organisme responsable de la recherche), contrairement aux premières.

Les traitements de données concernés par les manquements susvisés ayant cessé après les contrôles, la présidente de la CNIL a décidé d'adresser un simple rappel aux obligations légales à chacun des deux organismes, comme prévu par la loi « Informatique et Libertés ».

3. Point d'attention

L'analyse d'impact un outil qui contribue à la construction d'un traitement conforme au RGPD et respectueux de la vie privée. Cette analyse – en partie de nature technique – permet d'identifier des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, facilitant ainsi la détermination des mesures techniques et organisationnelles nécessaires pour protéger les données. Indépendamment de son caractère obligatoire pour certains traitements tels que ceux mis en œuvre dans le cadre de la recherche médicale, cette analyse d'impact est vivement recommandée dans l'optique de sécuriser les traitements.

A cet égard, il est rappelé, à toutes fins utiles, que la sécurité des données de santé, qui avait déjà été retenue comme thématique annuelle des contrôles de la CNIL en 2020 et en 2021, est une « *question récurrente* » que la CNIL rencontre dans un grand nombre de dossiers et qui concerne l'ensemble des établissements de santé.

En 2023, la sécurité des données sera encore au cœur des préoccupation de l'autorité de contrôle : « *Des vérifications ont déjà été engagées par la CNIL sur l'accès au dossier patient informatisé (DPI) en 2022 et se poursuivront en 2023. Ce choix fait notamment suite à des plaintes reçues par la CNIL qui dénoncent des accès par des tiers non autorisés à des DPI au sein d'établissements de santé. Les contrôles menés auront également pour objet d'examiner l'ensemble des mesures mises en place pour assurer la sécurité des données*. »[2]

[1] https://www.cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-deux-organismes-de-recherche-medicale-leurs-obligations-legales

[2] https://www.cnil.fr/fr/thematiques-prioritaires-de-controle-2023-cameras-augmentees-applications-mobiles-fichiers-bancaires#:~:text=En%202023%2C%20elle%20se%20concentrera,sant%C3%A9%20et%20les%20applications%20mobiles.

Alexandre FIEVEE

PANORAMA EUROPÉEN

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

Pas de données personnelles dans une thèse de médecine

GDPD (Italie), 24 novembre 2022

Un médecin a été sanctionné par l'autorité de contrôle italienne pour avoir publié dans sa thèse, accessible sur internet, des données non anonymisées.

Sous la supervision d'un psychiatre référent, un couple a réalisé une consultation auprès d'un interne en médecine se spécialisant en psychiatrie.

Le couple a, par la suite, appris de manière fortuite que ladite consultation, qui avait été relatée dans la thèse de l'interne, avait été publiée sur un site internet dédié aux publications scientifiques. Par ailleurs, la thèse comportait de nombreuses données personnelles les concernant, et notamment leur âge (ainsi que celui de leurs enfants), mais également leur profession, leurs histoires familiales respectives et de nombreux autres éléments d'ordre personnel. Seuls les noms avaient été pseudonymisés.

Le couple a déposé une plainte auprès de l'autorité de contrôle italienne qui a constaté que la thèse « *contenait les données personnelles (y compris des données de santé)* » du couple, et que le médecin « *avait effectué un traitement de données personnelles en violation [du RGPD]* ».

Pour sa défense, le médecin se prévalait de l'anonymisation des noms de famille. Mais l'autorité de contrôle a rappelé que le simple remplacement du nom de famille par un pseudonyme n'est pas une mesure appropriée pour garantir l'anonymisation des données à caractère personnel et, en tout état de cause, que le seul fait d'avoir eu recours à un psychiatre est déjà une donnée de santé.

Constatant (i) l'absence de base légale, conformément aux articles 6 et 9 du RGPD, et, à défaut (ii) l'absence d'anonymisation en bonne et due forme, l'autorité de contrôle italienne a infligé au médecin une amende de 1.000 euros.

Source : ici

Profiler une personne pour déterminer son risque de complication en cas de covid est illicite

GDPD (Italie), 15 décembre 2022

L'autorité de contrôle italienne a sanctionné une agence sanitaire italienne pour avoir établi un profil de risque de patients en cas de contraction de la covid-19 en méconnaissance de nombreux principes du RGPD.

Dans le but de mettre en œuvre *« des interventions préventives de prise en charge du patient »*, une agence sanitaire italienne a créé des *« profils de risques sanitaires » afin de « classer les patients considérés comme étant à risque ».*

Plus précisément, l'agence sanitaire a accédé à une base de données comportant les données de santé de près de 40 000 personnes et a effectué sur cette base un traitement algorithmique.

L'algorithme profilait les personnes et dressait une liste des patients les plus à risques en cas d'infection à la covid-19.

Alerté par l'existence de ce traitement, l'autorité de contrôle italienne a ouvert une enquête et considéré que le traitement était illégal car (i) violait le principe de licéité (article 5§1a du RGPD) et (ii) était réalisé en violation de l'interdiction de traiter des données de santé (article 9 du RGPD).

Plus encore, le responsable du traitement n'avait pas fourni aux personnes concernées les informations nécessaires (articles 12 à 14 du RGPD) et n'avait pas réalisé d'analyse d'impact relative à la protection des données personnelles, compte tenu notamment du grand nombre de personnes concernées par le traitement de données de santé (article 35 du RGPD).

En conséquence, l'autorité de contrôle a prononcé une amende de 55.000 € à l'encontre de l'agence sanitaire.

Source : ici

Prévention d'une fraude : pas de partage de données personnelles avec une autre société

IMY (Suède), 10 octobre 2022

L'autorité de contrôle suédoise a prononcé un rappel à l'ordre à l'encontre d'une société pour avoir partagé des données personnelles avec une autre société dans un objectif de prévention d'une fraude sans l'avoir mentionné dans sa politique de confidentialité.

Un consommateur suédois a réalisé un achat en ligne sur un site allemand. Considérant l'adresse électronique fournie comme frauduleuse et réalisant que le consommateur avait fourni un numéro de fax au lieu de son numéro de téléphone, l'entreprise éditant le site a procédé à des investigations pour s'assurer que l'adresse électronique était correcte.

Pour ce faire, elle a communiqué l'adresse électronique du consommateur à un prestataire de services anti-fraude.

Ayant eu connaissance de ce traitement, le consommateur allemand a déposé une plainte.

Au cours de son enquête, l'autorité de contrôle suédoise a d'abord constaté que l'entreprise n'avait pas suffisamment informé le consommateur, dans sa politique de confidentialité, de la possibilité que des données personnelles puissent être partagées avec un prestataire de services anti-fraude. Effectivement, ladite politique indiquait uniquement que les données pouvaient être transmises à des « *ressources externes* », cette information n'étant, selon l'autorité de contrôle, « *pas suffisamment spécifique pour satisfaire l'exigence de l'article 13* » du RGPD.

IMY. Integritetsskydds myndigheten

L'autorité de contrôle a ensuite considéré que la base légale sur laquelle s'appuyait la société, à savoir le « *respect d'une obligation légale* », n'était pas valable dès lors que, bien qu'une loi existait, les traitements effectués n'étaient pas « *nécessaires* ». En effet, « *l'entreprise aurait pu prendre des mesures moins coercitives* », par exemple en « *s'abstenant de traiter la commande jusqu'à ce que le consommateur la recontacte* » ou en envoyant une « *lettre* » ou un « *fax* ».

En revanche, l'autorité de contrôle a indiqué que « *l'intérêt légitime* » de la société aurait été une base légale valable pour justifier le traitement de données à caractère personnel à des fins de prévention de la fraude. Malheureusement, l'entreprise n'a pas utilisé cette base légale pour justifier la licéité de son traitement…

Compte tenu de ce qui précède, l'autorité de contrôle suédoise a prononcé un rappel à l'ordre à l'encontre de la société pour avoir traité les données personnelles du consommateur sans base légale et pour n'avoir pas fourni d'information suffisante sur (i) l'existence d'un transfert de données à caractère personnel à des fins de lutte contre la fraude et sur (ii) les destinataires de ces dernières.

Source : ici

Double peine pour un hôpital : ransomware et sanction de l'autorité de contrôle

CDP (Irlande), 23 janvier 2023

L'autorité de contrôle irlandaise a sanctionné un hôpital qui avait subi une attaque par ransomware, pour n'avoir pas mis en œuvre les mesures techniques et organisationnelles adéquates.

Un hôpital irlandais a subi une attaque informatique par ransomware qui a entraîné l'accès non autorisé, la modification et la destruction de données personnelles de 70 000 patients, incluant des données de santé. Malgré des sauvegardes quotidiennes, certaines de ces données personnelles n'ont pas pu être récupérées.

L'autorité de contrôle irlandaise, après avoir reçu la notification de la violation de données personnelles, a ouvert une enquête et a sollicité de l'hôpital la fourniture d'informations relatives aux mesures de sécurité mises en œuvre.

Elle a, dans un premier temps, considéré que « *le traitement des données à caractère personnel par l'hôpital présentait un risque élevé, tant en termes de probabilité que de gravité, pour les droits et libertés des personnes concernées* », en raison notamment de « *la quantité importante de données* », relevant de « *catégories particulières* » et des « *risques d'entrave à la fourniture de soins médicaux aux personnes concernées* ».

Elle a, dans un second temps, analysé en détail les « *mesures mises en œuvre par l'hôpital pour faire face aux risques* » et considéré ces dernières insuffisantes, dès lors que l'hôpital :

- n'appliquait pas immédiatement les correctifs de sécurité Windows ;
- effectuait une sauvegarde quotidienne de ses données sur un serveur local ;
- avait une politique de gestion des mots de passe inadaptée ;
- disposait d'un pare-feu mal configuré ;
- ne disposait d'aucun plan de continuité des activités.

Dans ce contexte, l'autorité de contrôle irlandaise a infligé à l'hôpital une amende de 460.000 €.

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 Paris) ou en visio-conférence.
Inscription et informations :