NEWSLETTER RGPD/DATA

NUMÉRO 49 ● DECEMBRE 2022

SOMMAIRE

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

ACTUALITE

LES ETATS-UNIS, BIENTOT RECONNUS PAYS « ADEQUAT »

La Commission européenne a annoncé, le 13 décembre 2022, avoir lancé le processus d'adoption d'une décision d'adéquation visant à régulariser les transferts de données personnelles de l'Union européenne vers les Etats-Unis.

Après le *Safe Harbor* et le *Privacy Shield*, mécanismes tous deux invalidés, la Commission pourrait adopter une nouvelle décision d'adéquation concernant les Etats-Unis.

Pour rappel :

- Le 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE) a, dans une décision « Schrems II », 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.
- Le 25 mars 2022, la présidente de la Commission européenne et le président des Etats-Unis ont annoncé avoir convenu d'un accord de principe sur un nouveau cadre de protection des données EU-US.
- Le 7 octobre 2022, le président des Etats-Unis a signé un décret présidentiel visant à renforcer les garanties portant sur les activités de renseignement des Etats-Unis. Selon un communiqué de la Commission européenne, ce décret présidentiel implémente l'accord de principe annoncé en mars 2022.
- Au lendemain de l'adoption de ce décret du 7 octobre 2022, la Commission avait annoncé amorcer (i) la préparation d'un projet de décision d'adéquation et (ii) le lancement de la procédure d'adoption.

Dernière actualité en date : le 13 décembre 2022, la Commission européenne a annoncé avoir lancé le processus tendant à l'adoption d'une décision d'adéquation concernant les transferts de données entre Union européenne et Etats-Unis.

Un projet de décision d'adéquation a d'ailleurs d'ores et déjà été rédigé, publié et soumis au CEPD pour avis.

Ce projet de décision prévoit notamment :

- que les sociétés américaines pourront bénéficier du mécanisme d'adéquation en s'engageant à se conformer à un ensemble d'obligations détaillées en matière de protection des données (exemple : supprimer les données personnelles lorsqu'elles ne sont plus nécessaires à l'objectif du traitement) ;
- plusieurs voies de recours accordées aux citoyens européens, dans l'hypothèse où leurs données personnelles seraient traitées en violation de ce cadre juridique, notamment la possibilité de saisir gratuitement des mécanismes indépendants de règlement des litiges et un groupe d'arbitrage ;

- un certain nombre de limitations et de garanties concernant l'accès aux données par les autorités publiques américaines, notamment à des fins de répression pénale et de sécurité nationale.

Une fois l'avis du CEPD rendu, la Commission européenne sollicitera l'approbation d'un comité composé de représentants des Etats membres de l'UE et permettra au Parlement européen d'exercer son droit de regard. La Commission européenne pourra, ensuite, procéder à l'adoption de la décision finale d'adéquation.

Une fois en vigueur, ce cadre juridique fera l'objet d'examens périodiques par la Commission européenne, en collaboration avec les autorités de contrôle européennes, afin de s'assurer de sa mise en œuvre pratique et de l'efficacité de son fonctionnement.

Source : ici

AMENDE CNIL DE 800.000 € A L'ENCONTRE DE DISCORD

Le 10 novembre 2022, la CNIL a condamné la société DISCORD INC. au paiement d'une amende administrative de 800.000 €, pour avoir notamment manqué à ses obligations en matière de « Privacy by default » et de conduite d'une analyse d'impact.

Discord est un logiciel de voix sur IP et de messagerie instantanée, permettant aux utilisateurs de créer des serveurs, ainsi que de salons textuels, vocaux et vidéos. Discord est édité par DISCORD INC.

La CNIL a effectué une mission de contrôle en ligne sur le site web « discord.com » et sur l'application mobile Discord, suivie d'une mission de contrôle sur pièces, au moyen d'un questionnaire transmis à DISCORD INC.

Suite aux réponses apportées par DISCORD INC., la CNIL a relevé les manquements suivants :

1. Manquement à l'obligation de définir et de respecter une durée de conservation des données proportionnées à la finalité du traitement.

DISCORD INC. conservait les données personnelles liées à un compte utilisateur jusqu'à la fermeture dudit compte, par l'utilisateur.

La CNIL y a vu un manquement au principe de limitation de la conservation. La durée choisie par DISCORD INC. divergeait des recommandations de la CNIL, telles que formulées dans son référentiel sur la gestion commerciale et la gestion des impayés du 3 février 2022, qui consistent à supprimer les comptes inactifs au bout de deux ans, sauf souhait contraire de l'utilisateur.

Pour la CNIL, « *la société ne saurait se prévaloir en l'espèce du maintien d'une relation contractuelle pour conserver indéfiniment des comptes d'utilisateurs totalement inactifs, mais qui ne se seraient pas désinscrits, dès lors que le compte a été créé gratuitement et qu'un utilisateur inactif qui souhaiterait utiliser à nouveau le service peut le faire en recréant un compte à tout moment* ».

2. Manquement à l'obligation d'information des personnes.

Ain de satisfaire aux exigences de l'article 13 du RGPD, DISCORD INC. avait publié une information quant à la durée de conservation des données personnelles des utilisateurs, dans les termes suivants :

> « *Nous conservons généralement les données personnelles le temps nécessaire aux fins définies dans ce document. Pour nous débarrasser des données personnelles, nous pouvons les rendre anonymes, les supprimer ou prendre d'autres mesures nécessaires. Il est possible que des données persistent quelque temps sous la forme de copies de sauvegarde ou à des fins commerciales.* »

Pour la CNIL, cette énonciation des durées de conservation était générique et n'était pas « *suffisamment explicite* », dans la mesure où elle ne comprenait « *ni durée précise, ni critères permettant de déterminer ces durées* ». Elle a donc relevé un manquement à l'obligation d'information des personnes.

3. Manquement à l'obligation de garantir la protection des données par défaut.

Le principe de « protection des données par défaut » impose de « *mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées* ».

La CNIL a relevé que, par défaut, lorsque l'utilisateur clique sur la croix de fermeture de l'application Discord, cette dernière est simplement mise en arrière-plan et n'est pas fermée : l'utilisateur est toujours en mesure de communiquer vocalement. Pour la CNIL, cela conduit à la communication de données personnelles à des tiers, alors que l'utilisateur est susceptible de penser « *en l'absence d'information spécifique suffisamment visible et claire, que leur collecte avait cessé lorsqu'il avait choisi de fermer la fenêtre de l'application* ». La CNIL a qualifié ce paramétrage de manquement à l'obligation de protection des données par défaut.

DISCORD INC. a, en tant qu'action corrective, mis en place une fenêtre « pop-up » apparaissant la première fois que l'utilisateur clique sur la croix et permettant de l'alerter sur le fait que l'application Discord est toujours en cours de fonctionnement.

4. Manquement à l'obligation de sécurité des données.

La CNIL a relevé qu'un mot de passe composé de six caractères incluant des lettres et des chiffres était accepté lors de la création d'un compte sur Discord. Elle a considéré que « *la robustesse des mots de passe admis par la société était trop faible, conduisant à un risque de compromission des comptes associés et des données à caractère personnel qu'ils contiennent* », relevant, ainsi, un manquement à l'obligation de sécurité des données.

5. Manquement à l'obligation de réaliser une analyse d'impact.

Le RGPD impose de réaliser une analyse d'impact lorsque le traitement de données est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques* ».

En l'espèce, la CNIL a considéré qu'au regard du nombre élevé d'utilisateurs de Discord en France, qui implique une « *collecte de données à large échelle* », et de l'utilisation du service par des enfants âgés de quinze ans, impliquant une « *collecte de données de personnes vulnérables* », la réalisation d'une analyse d'impact s'imposait à DISCORD INC.

Cette analyse d'impact n'ayant pas été réalisée, la CNIL a considéré que DISCORD INC. a méconnu ses obligations en la matière.

La CNIL a prononcé une amende administrative de 800.000 € à l'encontre de DISCORD INC., au regard, notamment, de sa « *situation financière* », des « *efforts réalisés par la société pour se mettre en conformité tout au long de la procédure* », ainsi que du fait que « *son modèle d'affaires n'est pas fondé sur l'exploitation des données à caractère personnel* ».

Source : ici

MICROSOFT 365 DANS LE VISEUR DES AUTORITES DE CONTROLE ALLEMANDES

Le comité des autorités de protection des données allemandes a entamé des discussions avec Microsoft afin d'obtenir de cette dernière qu'elle améliore la conformité de ses services Microsoft 365 au RGPD.

Le 22 septembre 2020, le comité fédéral des autorités de contrôles allemande (la « DSK ») a monté un groupe de travail chargé d'entamer des discussions avec Microsoft afin d'obtenir des améliorations quant à la conformité des services Microsoft 365 aux exigences du RGPD et de la décision Schrems II.

A l'issues de plusieurs entretiens entre Microsoft et le groupe de travail, les constatations, recensées dans un document publié le 24 novembre 2022, ont été les suivantes :

- Les finalités de traitement et les catégories de données personnelles traitées ne sont pas suffisamment décrites dans le cadre contractuel de Microsoft. Le groupe de travail suggère, sur ce point, d'utiliser l'annexe des clauses contractuelles types « article 28 » de la Commission européenne, ou encore d'intégrer au contrat le registre des activités de traitement du responsable du traitement.
- Le cadre contractuel de Microsoft ne distingue pas non plus suffisamment les traitements réalisés par Microsoft en qualité de sous-traitant et ceux réalisés en qualité de responsable du traitement, notamment « *à des fins commerciales légitimes* » ou bien à des fins de diagnostic, ni sur quelles bases légales se fondent ces traitements.
- Le cadre contractuel permet également à Microsoft de communiquer les données du responsable du traitement à des tiers, de façon plus large que ce qui est prévu par le RGPD, potentiellement en violation des articles 28 et 48 du RGPD.
- En cas de changement de sous-traitant, Microsoft envoi une information générale indiquant que des modifications sont prévues à ce sujet, sans préciser lesquelles. En comparaison, les clauses contractuelles types « article 28 » prévoient une information plus détaillée, incluant le nom, l'adresse et la personne de contact du sous-traitant ultérieur, ainsi qu'une description du traitement concerné.
- Le cadre contractuel, qui demeure non-exhaustif quant aux pays vers lesquels les données personnelles sont transférées, prévoit néanmoins la possibilité, pour Microsoft, de transférer des données à caractère personnel vers les Etats-Unis, en utilisant les clauses contractuelles types.

Il résulte des entretiens entre Microsoft et le groupe de travail qu'il n'est pas possible d'utiliser Microsoft 365 sans transférer de données personnelles vers les Etats-Unis. Par ailleurs, dans le cadre de ce transfert, les données restent lisibles par le destinataire, de sorte que ce transfert n'est pas conforme aux exigences de l'arrêt Schrems II.

Le DSK n'a pas précisé quelles suites il entendait donner à ce dossier.

Source : ici

CONSERVATION DES DONNEES DE CONNEXION AFIN DE LUTTER CONTRE LA CRIMINALITE GRAVE : LA CJUE CONFIRME ET RENFORCE SA POSITION

Dans un arrêt du 17 novembre 2022, la CJUE s'est à nouveau prononcée sur la question de la légalité de la conservation généralisée et indifférenciée des données de connexion à des fins de lutte contre la criminalité grave. Retour sur une décision qui ne laisse pas de place au doute.

Cette décision s'inscrit dans le cadre d'un litige pénal bulgare. Le parquet avait demandé au tribunal pénal l'autorisation d'accéder à des données de trafic et de localisation concernant des appels téléphoniques de personnes potentiellement impliquées dans une activité criminelle de distribution de cigarettes.

Le tribunal a accueilli favorablement cette demande en retenant notamment que l'activité en cause constituait une infraction grave commise intentionnellement et que le dossier mettait en évidence que les numéros de téléphone concernés ont pu être utilisés lors de l'exercice de cette activité.

Pour ce faire, la juridiction s'est basée sur la loi bulgare permettant une telle conservation de données.

La juridiction bulgare s'est interrogée toutefois sur la conformité de telles règles avec le droit de l'Union dans la mesure où la CJUE a déjà jugé qu'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, aux fins de la lutte contre la criminalité grave, n'est pas compatible avec le droit de l'Union.

La CJUE a ainsi été saisie notamment sur le point de savoir si (i) une limite de conservation des données dans le temps (6 mois) ou encore (ii) la mise en place de certaines garanties en matière de conservation et d'accès aux données concernées pourraient être compatibles avec le droit de l'Union, en particulier la Directive dite « Vie privée et communication » et la Charte des droits fondamentaux.

Dans sa décision, la CJUE a tout d'abord jugé que la conservation de données de connexion présente, en tout état de cause, un caractère grave. Selon la Cour, la conservation d'une quantité même limitée de ces données ou pour une période courte peut révéler des informations particulièrement précises sur la vie de l'utilisateur (par exemple : ses déplacements, les lieux qu'il fréquente, ses relations, etc.), En conséquence, la conservation de données de connexion limitée à une période de 6 mois est contraire au droit de l'Union (à noter que la CJUE avait déjà adopté une telle position de principe dans un arrêt du 20 septembre 2022 (affaires jointes C-793/19 et C-794/19)).

La CJUE a poursuivi en jugeant que la mise en place de garanties par une loi nationale, telles que (i) l'existence de règles claires et précises excluant un accès généralisé aux données conservées, (ii) des obligations à la charge des fournisseurs de services de communications électroniques pour assurer la sécurité et la protection des données ou encore (iii) la surveillance de la conservation des données par des autorités indépendantes, ne sauraient modifier un tel constat.

A cet égard, les juges européens ont précisé que cela ne remédie notamment pas à l'ingérence grave d'une telle conservation dans les droits fondamentaux, parmi lesquels le droit au respect de la vie privée. Aussi, la surveillance par une CNIL nationale, par exemple, ne permettrait pas de supprimer les risques liés à la conservation des données (obtenir des informations particulièrement précises sur la vie privée des personnes concernée).

La position de la CJUE est donc sans appel : une législation nationale ne peut prévoir, sauf à violer le droit de l'Union, préventivement, une conservation généralisée et indifférenciée de données de connexion, même avec une limite de conservation (6 mois) et des garanties en termes de conservation et d'accès aux données.

A noter que la CJUE a également indiqué dans cette décision que lorsque des autorités nationales compétentes en matière d'enquêtes pénales peuvent avoir accès à des données de connexion, les personnes concernées doivent en être informées et disposer d'une voie de recours en cas d'accès illégal à ces données.

Source : ici

LE NON-RESPECT DU RGPD QUALIFIE DE CONCURRENCE DELOYALE

Dans le cadre d'un contentieux relatif à la contrefaçon de marques et de brevets, une société a fait grief à une autre de ne pas respecter la législation relative à la protection des données, engendrant, selon elle, des actes de concurrence déloyale. Le Tribunal judiciaire de Paris a accueilli favorablement ce grief pour sanctionner la société concurrente.

La société « Plaisance Equipements », titulaire d'une marque et de brevets sur ses produits, a assigné (i) en contrefaçon de ses brevets et de sa marque et (ii) en concurrence déloyale, une société concurrente qui commercialisait sur son site web des produits appartenant à la société Plaisance Equipements.

Au titre de la concurrence déloyale, la société Plaisance Equipements considérait que « *le non-respect de la réglementation en vigueur par [la société concurrente] dans l'exercice de son activité commerciale […] induisait nécessairement un avantage concurrentiel indu […] générateur en lui-même, d'un trouble commercial impliquant nécessairement l'existence d'un préjudice* ».

Plus précisément, elle considérait que la violation de « *l'intégralité de la législation relative à la protection des données à caractère personnel au titre de la diffusion de son site internet [était constitutif] d'actes de concurrence déloyale par manquement à la loi, sur le fondement de l'article 1240 du Code civil* ».

Après s'être prononcée sur l'existence d'une contrefaçon, le Tribunal judiciaire a suivi les moyens invoqués par Plaisance Equipements.

Le Tribunal a, dans un premier temps, rappelé que la concurrence déloyale, fondée sur l'article 1240 du Code civil, « *consiste dans des agissements s'écartant des règles générales de loyauté et de probité professionnelle applicables dans les activités économiques et régissant la vie des affaires* ».

Rappelant, ensuite, la décision de la Cour de cassation selon laquelle « *constitue un acte de concurrence déloyale le non-respect d'une règlementation dans l'exercice d'une activité commerciale, qui induit nécessairement un avantage concurrentiel indu pour son auteur* », le Tribunal a constaté que la société concurrente procédait à « *une collecte de données à caractère personnel […] sans fournir aucune information sur les conditions de ce ou ces traitements et en se limitant en réalité à un paragraphe d'information dans l'onglet « ''mentions légales'' »* ».

Cette collecte de données personnelles n'était, selon le Tribunal, pas conforme à l'obligation d'assurer « *la confidentialité et la sécurité des données personnelles traitées* », ni à l'obligation de veiller « *à ce que ces données ne soient ni altérées ni communiquées à des tiers non autorisées* » dès lors qu'« *aucune charte de confidentialité [n'était] mise à la disposition du public* » pour informer les personnes concernées par ce traitement (le lien renvoyant à une page d'erreur).

Compte tenu de tout ce qui précède, et « *dans la mesure où tout manquement à la réglementation dans l'exercice d'une activité commerciale induit nécessairement un avantage concurrentiel indu pour son auteur* », le Tribunal a considéré que la société concurrente « *s'est rendue coupable d'acte de concurrence déloyale au préjudice de [Plaisance Equipements]* », et l'a condamnée à payer à la société Plaisance Equipements la somme de 15 000 euros.

Source : ici

DOCTRINE

RGPD

Le DPO : dans l'œil du cyclone ? (Première 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. Ce mois-ci, il se penche sur la question des fonctions du DPO, et plus particulièrement celle de son positionnement dans l'organisme (Première partie). Le mois prochain, il abordera la problématique de l'exercice effectif par le DPO de ses missions (Seconde partie).

Le CEPD a annoncé, en septembre dernier, que son action coordonnée 2022/2023 portera sur les problématiques liées à la désignation du DPO et son positionnement dans les organismes. 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 l'organisme, ses ressources, ses missions a été 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 deux problématiques en lien avec le DPO : (i) son association à toutes les questions relatives à la protection des données dans l'organisme et (ii) son positionnement dans celui-ci vis-à-vis notamment de la direction.

En effet, il ressort des termes de l'article 38-1 du RGPD que le responsable du traitement doit veiller à ce que le délégué à la protection des données soit « *associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel* ». Le CEPD considère, sur cette base, que l'organisme doit s'assurer notamment (i) que le DPO participe régulièrement aux réunions de l'encadrement supérieur et intermédiaire, (ii) que sa présence est effective lorsque des décisions ayant des implications en matière de protection des données sont prises et (iii) que l'avis du DPO est dûment pris en considération. Enfin, en application de l'article 38-3 du RGPD, le délégué à la protection des données doit faire « *directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant* ».

Les affaires

Dans plusieurs décisions rendues par l'autorité de contrôle luxembourgeoise, des organismes ont été sanctionnés pour ne pas avoir correctement associé le DPO aux problématiques « *RGPD* » de l'organisme. Tel a été le cas d'une société qui ne permettait pas à son délégué à la protection des données de participer au comité directeur de manière systématique[1]. Un organisme a été également sanctionné parce que le DPO ne pouvait intervenir, que sur invitation ou de manière ad hoc, aux différentes réunions et comités dans lesquels étaient discutés les projets ayant des impacts en matière de protection des données, et ce sans qu'aucune règle ou fréquence ne soit définie[2]. Un autre cas de sanction concerne un organisme qui autorisait l'accès du DPO au comité de direction et aux réunions de gestion de projets en fonction de l'ordre du jour[3] ou encore un responsable du traitement qui n'impliquait son DPO que de manière limitée, lorsque la direction en faisait la demande expresse[4]. Enfin, il a été reproché à un organisme de n'associer qu'indirectement le DPO groupe aux questions relatives à la protection des données puisque ce dernier ne faisait pas partie du comité « *RGPD* » organisé par les filiales et n'était informé des sujets qui y étaient discutés qu'à travers les procès-verbaux. Selon l'autorité de contrôle luxembourgeoise, il y avait

là un manquement aux dispositions de l'article 38 du RGPD puisque le DPO groupe n'était finalement pas informé et surtout pas consulté « *dès le stade le plus précoce possible* » de toutes les questions relatives à la protection des données. Non seulement le DPO doit pouvoir participer régulièrement aux réunions de l'encadrement supérieur et intermédiaire, mais il doit également pouvoir faire un rapport au niveau le plus élevé de la direction. Tel n'est pas le cas lorsqu'une telle faculté est conditionnée à l'existence et la démonstration d'un « *problème significatif* »[5], comme l'indique l'autorité luxembourgeoise de protection des données. Lorsque le délégué rend compte à une « *personne de contact* » et non directement à la direction générale, le manquement est également caractérisé, selon l'autorité belge[6]. En tout état de cause, il appartient à l'organisme de démontrer l'accès direct du DPO au plus haut niveau de direction, notamment lorsqu'il existe, dans les faits, un ou plusieurs niveaux hiérarchiques entre la direction et lui[7]. Cette démonstration est bien entendu plus aisée quand le DPO rapporte directement au comité de direction[8] ou au directeur général[9].

Quelles recommandations ?

Compte tenu de ce qui précède, il est vivement recommandé (i) d'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 et (ii) de lui donner un accès direct et non conditionné au niveau le plus élevé de la direction. De telles actions sont indispensables pour garantir l'exercice effectif par le DPO de ses missions notamment d'information et de conseil. Bien entendu, la mise en œuvre de ces actions doit être documentée au moyen de procédures, notes internes et comptes-rendus de réunions.

Alexandre FIEVEE
Avocat Associé

DERRIENNIC ASSOCIES

Notes

(1) CNPD, Délibération n°20FR/2021, 11 juin 2021.

(2) CNPD, Délibération n°41FR/2021, 24 octobre 2021.

(3) CNPD, Délibération n°40FR/2021, 27 octobre 2021.

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

(5) CNPD, Délibération n°20FR/2021, 11 juin 2021.

(6) APD, Décision 24/2021, 19 février 2021.

(7) CNPD, Délibération n°40FR/2021, 27 octobre 2021.

(8) APD, Décision 56/2021, 26 avril 2021.

(9) APD, Décision 117/2021, 22 octobre 2021.

PANORAMA EUROPÉEN

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

La perte d'un diplôme, par une école, constitutive d'un manquement à la sécurité

AZOP (Croatie), 31 mai 2022

L'autorité de contrôle croate a mis en demeure une école de prendre les mesures techniques et organisationnelles appropriées dans le but de prévenir toute nouvelle perte de document, après avoir constaté que l'école avait égaré le diplôme de master d'un ancien étudiant.

Un étudiant a demandé à son ancienne université de lui transmettre la copie de son diplôme de master.

Bien qu'ayant l'obligation de conserver une copie desdits diplômes, l'université a indiqué à l'étudiant que le document avait été perdu, probablement lors du récent déménagement dans ses nouveaux locaux.

Considérant cette perte comme un manquement au RGPD, l'étudiant a déposé une plainte auprès de l'autorité de contrôle.

Au cours de son enquête, cette dernière a considéré que l'école n'avait pas respecté le principe de protection par défaut (article 25 du RGPD), mais surtout qu'elle n'avait pas mis en œuvre les mesures techniques et organisationnelles (les mesures de sécurité) appropriées afin d'empêcher toute possibilité de perte ou de disparition de documents contenant des données personnelles (article 32 du RGPD).

Compte tenu de ce qui précède, l'autorité de contrôle a mis en demeure l'école de prendre les mesures techniques et organisationnelles appropriées dans le but de prévenir toute nouvelle perte de document.

Lien : ici

Aveu d'adultère : la diffusion de l'enregistrement n'est pas soumise au RGPD

DSB (Autriche), 8 juin 2022

L'autorité de contrôle autrichienne est venue rappeler les contours de « l'exception domestique », posée à l'article 2 du RGPD en rejetant une plainte adressée à l'encontre d'un individu qui avait transmis l'enregistrement d'une conversation téléphonique privée.

Dans le cadre d'une discussion avec un ami, une femme avait avoué avoir trompé son mari et avoir dû subir un avortement.

Cet ami avait enregistré, sur WhatsApp, la discussion au cours de laquelle ces deux évènements étaient abordés et avait transmis l'enregistrement au mari trompé ainsi qu'à deux autres personnes de son entourage.

Considérant l'enregistrement comme contraire au RGPD, la femme a déposé une plainte devant l'autorité de contrôle autrichienne.

Rappelant les termes de l'article 2 du RGPD selon lesquels « *Le [RGPD] ne s'applique pas au traitement de données à caractère personnel effectué […] par une personne physique dans le cadre d'une activité strictement personnelle ou domestique* », l'autorité de contrôle a considéré qu'« *aucun élément n'indique que ce traitement de données ait un quelconque lien avec une activité professionnelle ou économique* et *qu'il n'a été réalisé et transmis qu'aux fins d'apporter la preuve des manquements de la femme* ».

Par conséquent, l'autorité, qui a estimé que le RGPD ne s'appliquait pas au traitement litigieux, a rejeté la plainte.

Source : ici

Le renvoi vers un outil d'accès à distance aux données personnelles est suffisant

AEPD (Espagne), 26 octobre 2022

L'autorité de contrôle espagnole a rejeté la plainte du client d'une banque en considérant que le droit d'accès de ce dernier était satisfait dès lors que la banque l'a renvoyé vers un système d'accès à distance de ses données personnelles.

Un client avait exercé, dans des termes généraux, son droit d'accès auprès de sa banque.

La banque avait répondu à la demande en fournissant les données personnelles contenues dans son fichier client, mais n'avait pas fourni le détail des transactions financières. Elle avait cependant rappelé (i) qu'elle restait à disposition du client pour apporter des précisions et (ii) que le client pouvait, dans le cadre de son contrat et de l'option « *banque à distance* », consulter et vérifier à tout moment ses différentes transactions financières.

Considérant que sa banque n'avait pas suffisamment répondu à la demande de droit d'accès (dès lors qu'il n'a pas obtenu le détail de ses transactions financières), le client a déposé une plainte auprès de l'autorité de contrôle.

Au cours de son enquête, l'autorité de contrôle a rappelé que :

- D'une part, « *lorsque le responsable du traitement traite un grand nombre de données relatives à la personne concernée et que le droit d'accès est exercé sans précisions, le responsable du traitement peut demander de préciser [la requête]* ».
- D'autre part, « *le droit d'accès est réputé satisfait lorsque le responsable du traitement fournit à la personne concernée un système d'accès à distance, direct et sécurisé aux données personnelles* ». Plus précisément, le fait pour le responsable du traitement d'informer sur la manière dont la personne concernée peut accéder aux données est suffisant pour que la demande d'accès soit réputée satisfaite.

Compte tenu de ce qui précède et constatant (i) que la demande de droit d'accès exercée était « *générique* » et (ii) que la banque a répondu à la personne concernée en lui fournissait les données contenues dans son fichier client et en l'informant de la possibilité de visualiser et vérifier à tout moment les transactions financières par le biais du support à distance, l'autorité de contrôle a considéré que le responsable du traitement avait correctement répondu à la demande de droit d'accès et a rejeté la plainte du client.

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

Source : ici

Envoi d'une invitation à une personne décédée

GPDP (Italie), 15 septembre 2022

L'autorité de contrôle italienne a sanctionné une région pour n'avoir pas respecté le principe d'exactitude en envoyant une invitation à une personne décédée.

Une région, par l'intermédiaire de son autorité sanitaire locale, avait transmis à une fille décédée une invitation à participer au programme de dépistage du cancer du col de l'utérus.

Considérant cette invitation comme violant le RGPD, la mère de la personne concernée avait déposé une plainte auprès de l'autorité de contrôle italienne.

Au cours de son enquête, cette dernière, après avoir qualifié les données personnelles traitées de données de santé a, tout d'abord considéré que la base légale utilisée par la Région (l'existence d'un soi-disant contrat) était inexacte. En réalité, la base légale applicable était, d'une part, le « *motif d'intérêt public important* » et, d'autre part, « *la médecine préventive et les diagnostics médicaux* » (article 9§2 g et h)

Ensuite, l'autorité de contrôle a considéré que les personnes concernées n'étaient pas suffisamment informées ou obtenaient des informations erronées lors de l'adhésion au programme de dépistage du cancer. Effectivement, (i) des contradictions et erreurs étaient présentes sur les droits des personnes et la possibilité de retrait du consentement et (ii) des informations étaient manquantes, comme la durée de conservation des données.

Enfin, et surtout, l'autorité de contrôle a rappelé que « *le responsable du traitement doit veiller à ce que les données soient exactes et, si nécessaire, mises à jour, en prenant toutes les mesures raisonnables pour effacer ou rectifier en temps utile les données inexactes au regard des finalités pour lesquelles elles sont traitées (principe d'"exactitude")* ».

Or, en l'espèce, force est de constater que les mesures adoptées par la région n'ont pas permis de garantir l'exactitude des données de la fille et que le fait que cette dernière, décédée depuis de nombreuses années, ait reçu une invitation montre que les mesures n'étaient pas adaptées.

En conclusion, le traitement a été déclaré non conforme au RGPD dès lors que les données personnelles ont été traitées (i) en violation des principes de licéité, loyauté et transparence et du principe d'exactitude des données (article 5 du RGPD), (ii) sans base juridique valable (article 6 du RGPD) et (iii) sans fourniture d'informations aux personnes concernées (article 12 du RGPD).

Compte tenu de tout ce qui précède, l'autorité de contrôle a infligé une amende de 100 000 € à la région et l'a mise en demeure d'identifier les finalités et bases légales applicables (pour pouvoir informer au mieux les personnes concernées) ainsi que de respecter le principe d'exactitude en modifiant et complétant les informations erronées dans un délai de 90 jours.

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 :