NEWSLETTER RGPD/DATA

NUMÉRO 67 ● 2025

ACTUALITÉS DU CABINET P. 9

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

SOMMAIRE

ACHAT D'ALCOOL : LA VERIFICATION DE L'AGE PEUT-ELLE ETRE SYSTEMATIQUE ?

L'autorité de contrôle hongroise a sanctionné ALDI pour avoir contrôlé si les clients achetant des boissons alcoolisées étaient majeurs, en violation du RGPD.

Des contrôles de la majorité contestés

L'autorité de contrôle hongroise a reçu plusieurs plaintes dirigées contre la chaîne de supermarchés ALDI.

Les personnes concernées se plaignaient de devoir systématiquement justifier de leur majorité lors de l'achat de boissons alcoolisées. Les plaintes étaient les suivantes :

- Des personnes ont déclaré avoir dû indiquer leur date de naissance au caissier ;
- D'autres ont constaté que le caissier enregistrait leur date de naissance sur le logiciel de caisse ;
- D'autres, encore, indiquaient que les politiques de vérification de l'identité n'étaient pas identiques entre les magasins, et qu'aucune information n'était fournie sur le traitement ;
- Enfin, des personnes, dont une âgée de 70 ans, se plaignaient d'avoir dû prouver leur majorité, alors que celle-ci était évidente.

Des contrôles de la majorité contraires au RGPD

L'autorité de contrôle hongroise a considéré que la chaîne de supermarchés avait enfreint de nombreuses dispositions du RGPD :

- Le fait de ne pas avoir informé les personnes concernées sur le traitement viole le principe de transparence posé aux articles 12 et 13 du RGPD ;
- Le fait d'avoir demandé aux personnes concernées d'indiquer leur date de naissance à l'oral a été considéré comme une violation des exigences en matière de sécurité, posées à l'article 32 du RGPD ;
- Le fait d'enregistrer, sur le logiciel de caisse, la date de naissance des clients a, dans un premier temps, été considéré comme un traitement contraire au principe de minimisation, posé à l'article 5§1 c) du RGPD (l'autorité de contrôle a, dans son second temps, modifié sa décision en indiquant que l'enregistrement de la date de naissance n'était pas un traitement de données personnelles car les personnes concernées n'étaient pas identifiées ou identifiables) ;
- Enfin, le fait de demander aux caissiers de vérifier de manière systématique l'âge des personnes achetant de l'alcool, alors même que certaines d'entre-elles étaient « manifestement âgées de plus de 18 ans », est contraire aux principes de licéité et de minimisation, posés respectivement aux articles 6 et 5§1 c) du RGPD : la vérification de la majorité ne devant être réalisée, selon la loi hongroise, qu'« en cas de doute ».

Compte tenu de ce qui précède, l'autorité de contrôle hongroise a infligé à ALDI une amende de près de 200 000 euros.

Source : ici

COMMENT OBTENIR L'ANNULATION D'UNE DECISION DE CLOTURE DE PLAINTE DE LA CNIL ?

Le 30 décembre 2024, le Conseil d'Etat a statué sur une demande d'annulation d'une décision de clôture de plainte rendue par la CNIL.

Une plainte CNIL vite clôturée

Un particulier a introduit une plainte auprès de la CNIL, contre la Caisse primaire d'assurance maladie (CPAM), relative à l'utilisation de pixels de suivi et de liens traçants dans des communications électroniques.

La CNIL a adressé à la CPAM un courrier rappelant les règles applicables en matière de lecture et d'écritures d'informations dans un terminal et l'enjoignant à s'y conformer, puis a immédiatement clôturé la plainte.

Des motifs de nullité limités

Le particulier a demandé au Conseil d'Etat d'annuler la décision de clôture et d'ordonner à la CNIL de rouvrir la plainte.

Le Conseil d'Etat a indiqué que la CNIL dispose d'un large pouvoir d'appréciation pour décider des suites à donner à une plainte : « *Il appartient à la CNIL de procéder, lorsqu'elle est saisie d'une plainte ou d'une réclamation tendant à la mise en œuvre de ses pouvoirs, à l'examen des faits qui en sont à l'origine et de décider des suites à leur donner. Elle dispose, à cet effet, d'un large pouvoir d'appréciation et peut tenir compte de la gravité des manquements allégués au regard de la législation ou de la réglementation qu'elle est chargée de faire appliquer, du sérieux des indices relatifs à ces faits, de la date à laquelle ils ont été commis, du contexte dans lequel ils l'ont été et, plus généralement, de l'ensemble des intérêts généraux dont elle a la charge.* »

Le Conseil d'Etat a également rappelé qu'une décision de la CNIL peut être annulée par un juge pour excès de pouvoir, si un motif le justifie : « *L'auteur d'une plainte peut déférer au juge de l'excès de pouvoir le refus de la CNIL d'y donner suite. Il appartient au juge de censurer celui-ci, le cas échéant, pour un motif d'illégalité externe et, au titre du bien-fondé de la décision, en cas d'erreur de fait ou de droit, d'erreur manifeste d'appréciation ou de détournement de pouvoir*. »

Une décision exempte de motif d'annulation

En l'espèce, la CNIL a demandé à la CPAM de se mettre en conformité, décision qui n'est entachée d'aucun des motifs d'annulation.

Le Conseil d'Etat a donc rejeté la requête du particulier et en a profité pour rappeler que la décision de clôture ne fait pas obstacle, « *s'il apparaissait ultérieurement que le manquement n'a pas été corrigé* », au dépôt d'une nouvelle plainte.

Source : CE 30 décembre 2024 n°492106

COLLECTE DE LA MENTION « MONSIEUR » OU « MADAME » CONTRAIRE AU PRINCIPE DE MINIMISATION

De nombreux organismes, qu'ils soient publics ou privés, collectent la civilité de leurs usagers/clients en la limitant généralement à la mention « Monsieur » ou « Madame ». Cette pratique, devenue « banale » est-elle conforme au RGPD et, en particulier, au principe de minimisation ? La CJUE a récemment répondu à cette problématique par la négative.

Pour mémoire, l'article 5 c) du RGPD prévoit que les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation).

Une association de lutte contre les discriminations a considéré que SNCF Connect a violé ce principe de minimisation en collectant, systématiquement, la civilité de ses clients via la mention « Monsieur » ou « Madame » dans le cadre de l'achat de billets en ligne. En effet, selon l'association, cette civilité – correspondant à une identité de genre - n'apparaît pas nécessaire à un tel achat.

A la suite du rejet de sa plainte par la CNIL, l'association a porté l'affaire devant le Conseil d'Etat. Ce dernier a saisi la CJUE afin d'avoir des éclairages sur la licéité d'une telle pratique visant « *à permettre une communication commerciale personnalisée à l'égard de ces clients, conformément aux usages couramment admis en la matière* ».

La position de la CJUE est claire : « *l'identité de genre du client n'est pas une donnée nécessaire pour l'achat d'un titre de transport* ». Aussi, « *la collecte de données relatives à la civilité des clients n'est pas objectivement indispensable, en particulier, lorsqu'elle a pour finalité une personnalisation de la communication commerciale* ». En effet, selon la Cour, la SNCF aurait pu choisir de communiquer en recourant à « *des formules de politesse génériques, inclusives et sans corrélation avec l'identité de genre présumée des clients* », choix « *praticable et moins intrusi*[f] ».

Cette solution a une portée particulièrement large qui dépasse le secteur du transport. Tout organisme doit faire preuve d'une particulière vigilance lorsqu'il collecte, de façon obligatoire, des données de civilité, à partir du moment où elles ne sont pas strictement nécessaires au traitement en cause. La personnalisation d'une communication, en particulier, dictée par les usages ou la politesse ne suffira pas à justifier le traitement de telles données. Un audit de conformité de vos formulaires de collecte est à mener sans plus attendre…

Source : ici

LE GUIDE DE LA CNIL SUR L'ANALYSE D'IMPACT DES TRANSFERTS DE DONNEES

Le 31 janvier 2025, la CNIL a publié la version finale de son guide sur les analyses d'impact des transferts de données hors UE/EEE, qui implique une charge de travail conséquente pour qui procède à ce type de transferts.

Selon le RGPD, lorsqu'un organisme exporte des données personnelles en dehors de l'UE, il doit, selon l'outil de transfert auquel il a recours, évaluer le niveau de protection des données offert par le pays de destination afin de déterminer si, au regard des lois et pratiques de ce pays, l'implémentation de mesures supplémentaires s'impose.

La CNIL a publié un guide afin d'aider les organismes à procéder à cette évaluation, dénommée « *analyse d'impact des transferts de données* » ou « *AITD* ».

Qui doit réaliser une AITD ?

Selon le guide de la CNIL, une AITD doit être réalisée par l'exportateur de données soumis au RGPD, « *qu'il soit responsable du traitement ou sous-traitant* », transférant des données personnelles hors UE/EEE, sauf si le transfert se fonde sur une décision d'adéquation ou l'une des dérogations listées à l'article 49 du RGPD.

Lorsqu'un responsable du traitement dans l'UE, fait appel à un sous-traitant dans l'UE qui procède à un transfert hors UE/EEE de données personnelles, c'est bel et bien le sous-traitant qui doit réaliser l'AITD. Dans cette hypothèse, le responsable du traitement doit vérifier l'AITD et, si nécessaire, la compléter.

La réalisation d'une AITD s'impose donc dans un grand nombre de cas et son périmètre peut s'avérer particulièrement large, puisque l'ensemble des flux de données, y compris les transferts ultérieurs, doit être pris en compte.

Comment réaliser une AITD ?

L'AITD doit, selon la CNIL, être réalisée en six étapes :

- Etape 1 : décrire le transfert ;
- Etape 2 : identifier et documenter l'outil d'encadrement du transfert ;
- Etape 3 : évaluer la législation et les pratiques en vigueur dans le pays de destination, ainsi que l'efficacité de l'outil de transfert ;
- Etape 4 : recenser les mesures de sécurité techniques, contractuelles et organisationnelles permettant d'assurer un niveau de protection des données suffisant et identifier les mesures supplémentaires qui doivent être mises en œuvre pour assurer un niveau de protection « essentiellement équivalent » à celui de l'EEE ;
- Etape 5 : mettre en œuvre les mesures supplémentaires qui s'imposent, au moyen d'un plan d'action ;
- Etape 6 : réévaluer à intervalles appropriés le niveau de protection et suivre les développements potentiels qui pourraient l'affecter.

Ce travail nécessite, en particulier à l'étape 3, de s'intéresser de près à la législation et aux pratiques du pays de destination (textes applicables en matière de protection des données, droits des personnes concernées, lois permettant aux autorités publiques d'obtenir la divulgation de données, etc.).

La CNIL ne mentionne pas de ressource susceptible d'aider le responsable du traitement dans cette tâche, exceptée l'assistance du sous-traitant importateur, qui peut être sollicitée de la réalisation de l'AITD. En effet, le sous-traitant est tenu, selon l'article 28 du RGPD, de transmettre au responsable du traitement les informations permettant de démontrer le respect des obligations qui lui incombent.

Source : ici

DOCTRINE

RGPD

Accès d'un ex-salarié à ses données : l'employeur peut refuser

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les différentes autorités de contrôle nationales au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question de savoir si un employeur peut opposer le respect des droits et libertés d'autrui pour ne pas faire droit à une demande de droit d'accès émanant d'un ancien salarié contre lequel il est en litige.

En application de l'article 15 du RGPD, le droit d'accès permet à toute personne de savoir si des données personnelles la concernant sont traitées par un organisme déterminé, responsable du traitement, et d'en obtenir une copie dans un format compréhensible. Il doit être précisé que l'exercice de ce droit n'est pas conditionné, ce qui signifie que la personne concernée n'a pas à motiver sa demande. Par ailleurs, et selon la CJUE[1], les motifs qui animent la personne concernée sont indifférents, alors même qu'en application du considérant 63 du RGPD, la raison d'être de ce droit serait de permettre aux personnes concernées « *de prendre connaissance du traitement et d'en vérifier la licéité* ».

Ainsi, une personne peut exercer ce droit, comme le confirme la Cnil, « *en parallèle d'une procédure contentieuse (devant le conseil des prud'hommes par exemple) (...) en cours* »[2], dans l'optique d'obtenir la copie des données la concernant, que détient son employeur.

Toutefois, l'exercice de ce droit ne doit pas porter atteinte, selon les termes du paragraphe 3 de l'article 15 susvisé, « *aux droits et libertés d'autrui* », ce qui inclut le « *secret des affaires* » et la « *propriété intellectuelle* ». Selon le CEPD, ces droits et libertés explicitement mentionnés doivent être considérés comme de simples exemples, car, en principe, tout droit ou liberté fondé sur la législation de l'Union ou d'un État membre est susceptible d'être invoqué, tels que le droit à la protection des données ou encore le secret des correspondances. C'est en application de cette limite – le respect des « *droits et libertés d'autrui* » - que la juridiction administrative d'appel autrichienne a fait échec à une demande de droit d'accès émanant d'un salarié à l'encontre de son ancien employeur.

L'affaire[3]

Une personne, en litige contre son ancien employeur, avait déposé plainte auprès de l'autorité autrichienne de protection des données, au motif que la réponse à sa demande de droit d'accès était incomplète. Si l'employeur avait, en effet, transmis un grand nombre de données, il reconnaissait aussi que cette transmission avait été limitée aux seules données qui ne portaient pas atteinte aux droits et libertés d'autrui et notamment celles qui n'entravaient pas la procédure judiciaire en cours. L'employeur avait ainsi écarté notamment les « *échanges de courriels et prises de position* » concernant cet ancien salarié.

L'autorité autrichienne de protection des données a donné gain de cause à l'employeur, considérant que : « *Le droit d'obtenir une copie ne doit pas porter atteinte aux droits et libertés d'autres personnes. Par conséquent, le refus de fournir une copie des données serait justifié si les intérêts de la personne concernée ou de tiers en matière de confidentialité l'emportaient sur l'intérêt du plaignant à obtenir des informations. Comme il ressort des constatations, une procédure civile est en cours et il convient de reconnaître à [l'employeur] un intérêt à la confidentialité d'éventuels moyens de preuve, d'autant plus qu'il y aurait lieu de craindre une détérioration de sa position en justice. Une copie des dossiers n'est donc pas couverte par le droit d'accès.* »

L'ancien salarié a fait appel de cette décision devant le tribunal administratif fédéral autrichien. La juridiction a rejeté l'intégralité de ses prétentions, retenant d'abord que les éléments litigieux – « *échanges de courriels et prises de position* » -, dont le requérant demandait une copie, font partie intégrante de la procédure en cours entre les parties en présence. Elle a ensuite estimé que, dans un tel contexte, l'employeur fait valoir un intérêt légitime « *au maintien du secret* ». Ainsi, « *l'obtention d'informations renforçant la procédure du requérant va au-delà de l'objectif de protection de la règlementation* » et « *l'intérêt de [l'employeur] à la confidentialité des historiques de courriels et des prises de position susmentionnés l'emporte sur l'intérêt du requérant* ».

Quelles recommandations ?

Dans un article précédent[4], nous nous demandions, à la lumière de la décision de la CJUE susvisée, s'il était encore possible de s'opposer à une demande de droit d'accès reposant sur une autre motivation que celle d'apprécier la licéité d'un traitement. Nous en avions conclu qu'il serait désormais difficile de considérer comme abusive une demande de droit d'accès reposant sur des motifs autres que la vérification de cette licéité. Les personnes concernées pouvaient donc formuler des demandes de droit d'accès à tout va et quel qu'en soit le motif. Sauf à invoquer le secret des affaires, un droit de propriété intellectuelle ou encore le secret des correspondances, un employeur se devait de communiquer à son salarié toutes les données le concernant dont il dispose, y compris en parallèle d'une procédure judiciaire en cours, y compris pour alimenter le dossier « *juridique* » de ce dernier.

La décision du tribunal administratif fédéral autrichien relance incontestablement le débat (i) en reconnaissant un droit « *au secret* » pour l'organisme, mais aussi (ii) en affirmant que « *l'obtention d'informations renforçant la procédure du requérant va au-delà de l'objectif de protection de la règlementation* » et (iii) en faisant prévaloir l'intérêt de l'organisme à la confidentialité de certaines données sur l'intérêt du requérant.

L'organisme ne doit donc plus, pour se défendre d'une demande de droit d'accès notamment dans un contexte judiciaire avec la personne concernée, invoquer le caractère abusif de la demande eu égard aux motifs qui animent cette dernière, mais invoquer son propre droit au secret, son intérêt à préserver la confidentialité de certaines données.

Alexandre FIEVEE
Avocat Associé
DERRIENNIC ASSOCIES

Notes

(1) CJUE, C-307/22, 26 octobre 2023.

(1) https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces

(1) Tribunal administratif fédéral autrichien, W137 2278780-1, 8 juillet 2024.

(1) « Demandes de droit d'accès abusives : stop ou encore ? », Expertises, décembre 2023, Alexandre FIEVEE.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info

ACTUALITÉS DU CABINET

DERRIENNIC ASSOCIÉS PROPOSE UN PROGRAMME DE FORMATION DE 35 HEURES POUR LA PRÉPARATION À LA CERTIFICATION DPO

OBJECTIFS

1/ Acquérir les compétences, les connaissances et le savoir-faire attendus par la CNIL et permettre au collaborateur de se présenter à l'examen de certification en maximisant ses chances de succès.
2/ Indépendamment de la certification, la formation permet à l'apprenant de se familiariser avec la matière et d'acquérir les compétences, les connaissances et le savoir-faire pour :

- analyser une situation impliquant un traitement de données personnelles ;
- définir et appréhender les problématiques, les enjeux et les risques qui en découlent ;
- prendre les décisions qui s'imposent en concertation avec l'équipe « DPO ».

CONTENU DE LA FORMATION

Partie 1 : Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité
Partie 2 : Responsabilité (Application du principe d'« Accountability »)
Partie 3 : Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

COÛT

4.000 € HT/personne

INTERVENANT

Alexandre FIEVEE
Avocat Associé
01.47.03.14.94
afievee@derriennic.com

CLASSEMENTS
Alexandre Fievee figure dans le classement BestLawyers dans la catégorie « *Information Technology Law* » (2024).

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

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

RENSEIGNEMENTS PRATIQUES
Prochaine session en 2025 :
Sur demande.
Lieu de la formation :
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.
Inscription et informations :
afievee@derriennic.com