NEWSLETTER RGPD

NUMÉRO 37 • NOVEMBRE 2021

ACTUALITE DU CABINET

FORMATION A LA PREPARATION A LA CERTIFICATION « DPO ».

Le cabinet organise régulièrement des programmes de formation visant à la préparation des apprenants à l'examen de certification « DPO ».

Retrouvez notre programme à la fin de notre newsletter **P.11**

SOMMAIRE

LA CNIL PUBLIE SON GUIDE PRATIQUE SUR LE DPO

Le 16 novembre 2021, la CNIL a publié un guide dédié au délégué à la protection des données (ou « data protection officer », DPO), regroupant « les principales connaissances utiles et bonnes pratiques pour aider les organismes et accompagner les DPO déjà en poste ».

L'article 37 du Règlement général sur la protection des données 2016/679 (« RGPD ») impose aux responsables du traitement et aux sous-traitants de désigner un DPO, lorsqu'ils réalisent certaines activités de traitement. Dans les hypothèses où la désignation d'un DPO ne serait pas obligatoire, la CNIL recommande, toutefois, aux organismes rencontrant « *des problématiques relatives à la protection des données personnelles* », de procéder à une telle désignation.

Ce DPO peut faire parti de l'entreprise, ou bien constituer une ressource externe, telle qu'un avocat.

La CNIL a organisé son Guide pratique RGPD sur le délégué à la protection des données en quatre parties :

- Le rôle du DPO ;
- La désignation du DPO ;
- L'exercice de la fonction du DPO ;
- L'accompagnement du DPO par la CNIL.

Le **rôle du DPO** inclut le contrôle de l'effectivité des règles, qui prend la forme de vérifications organisées par le DPO (« audit interne ou relai interne ») ou menées par le DPO personnellement, en collaboration avec les autres fonctions clefs telles que le RSSI. Cette mission de contrôle doit, selon la CNIL, « *s'accompagner d'un suivi du plan d'actions correctrices et évolutives* ».

L'objet de ces contrôles ou audits peut consister en :

> *« - des vérifications de l'exactitude des informations contenues dans le registre des traitements mis en œuvre par l'organisme (inventaire des activités de traitement, périmètre des finalités, personnes concernées, nature des données traitées, destinataires et éventuels transferts hors de l'Union Européenne, durées de conservation, mesures de sécurité) ;*
>
> *- des vérifications de la conformité des traitements les plus sensibles, en prenant en compte les analyses d'impact effectuées (notamment s'agissant de la mise en œuvre des mesures censées diminuer la vraisemblance et la gravité des risques) ;*
>
> *- la mise en place d'outils de suivi et de contrôle de l'utilisation des traitements (analyse de logs, détection de données interdites, vérification du respect des durées de conservation, etc.) ;*
>
> *- un contrôle de l'effectivité des mesures techniques et organisationnelles de protection des données que l'organisme s'est engagé à mettre en œuvre* ».

La CNIL précise par ailleurs, sur le sujet de la priorisation des missions du DPO, que « *le niveau de vigilance et de moyens doit être d'autant plus fort que les risques présentés par les traitements sont importants (suivi rigoureux des traitements de données sensibles, formation de collaborateurs particulièrement impliqués, audit interne sur les mesures de sécurité, etc.)* ».

La **désignation du DPO** doit, selon la CNIL, faire l'objet d'actions de communication (par exemple via une note d'information) visant à apporter de la « *visibilité à la fonction et aux coordonnées du DPO au sein de l'organisme* ».

S'agissant de **l'exercice de ses fonctions**, le DPO doit être associé, le plus tôt possible, à toutes les questions relatives à la protection des données.

La présence du DPO doit être recommandée lorsque des décisions en matière de protection des données sont prises. Le DPO doit être en mesure de dialoguer et de travailler avec les fonctions jouant un rôle important dans la protection des données.

L'accès aux données et aux opérations de traitement doit lui être facilité.

Enfin, s'agissant de **l'accompagnement du DPO par la CNIL**, cette dernière rappelle que le DPO peut utiliser ses modèles et autres outils d'aide à la mise en conformité, recourir à son standard téléphonique, ainsi qu'aux outils de formation de la CNIL.

Lien vers le guide de la CNIL : https://www.cnil.fr/sites/default/files/atoms/files/guide_pratique_rgpd_-_delegues_a_la_protection_des_donnees.pdf

LA CNIL PRONONCE UNE SANCTION D'UN MONTANT DE 400 000 EUROS A L'ENCONTRE DE LA RATP

Par une délibération en date du 29 octobre 2021, la CNIL a prononcé une sanction à l'encontre de la RATP d'un montant de 400.000 euros au regard de plusieurs manquements au RGPD.

La RATP est un établissement public à caractère industriel et commercial, entité mère du groupe RATP, qui employait en 2019 environ 65.000 salariés.

Le 13 mai 2020, la CNIL a été saisie d'une plainte d'une organisation syndicale portant sur un fichier d'évaluation des agents de la RATP, constitué dans le cadre de la procédure d'avancement de carrière des agents de centre de bus. Selon l'organisation syndicale, le fichier en cause contenait un certain nombre de catégories de données à caractère personnel qui lui confèreraient un caractère illicite, voire discriminatoire.

Le 18 mai suivant, la RATP a notifié à l'autorité une violation de données à caractère personnel. La RATP faisait état d'une violation qui aurait consisté en l'utilisation d'un fichier contraire aux dispositions du RGPD dans le cadre des commissions de classement des agents du département BUS (commissions visant à établir quels agents bénéficient d'un avancement), entraînant la perte de confidentialité de données à caractère personnel.

A l'issue de contrôles sur pièces et sur place dans trois centres de bus, la CNIL a retenu plusieurs manquements au RGPD.

1. <u>Sur le manquement à la minimisation des données</u>

L'article 5.1.c du RGPD prévoit le principe de minimisation des données selon lequel les données à caractère personnel doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

La CNIL a retenu un manquement à l'article du RGPD en raison d'une collecte de données non nécessaire puisque des fichiers d'aide à la décision, constitués dans le cadre de la procédure d'avancement de carrière des agents de centre de bus, faisaient figurer le nombre de jours de grève exercés par les agents durant les années concernées par l'évaluation.

Or, la CNIL a retenu que l'utilisation de telles données n'était pas nécessaire pour atteindre les objectifs visés dans le cadre de la préparation des commissions de classement. Selon la Commission, l'indication du nombre total de jours d'absence suffisait, sans qu'il ne soit nécessaire de rentrer dans le détail en distinguant les jours liés à l'exercice du droit de grève.

2. Sur le manquement à la limitation de la durée de conservation des données

L'article 5.1.e du RGPD impose la limitation de la conservation des données « *pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

L'autorité de contrôle a considéré que la RATP a méconnu ses obligations au regard de l'article du RGPD précité puisque :

- Tout d'abord, concernant des données figurant sur une application utilisée pour le traitement et la gestion des ressources humaines, la CNIL a constaté que les données étaient conservées durant six ans en base active sans qu'une approche différenciée et adaptée de conservation des données ne soit mise en œuvre au regard des finalités précises pour lesquelles sont traitées les données.

- Ensuite, concernant les fichiers de préparation des commissions de classement, la CNIL a relevé que la durée de conservation prévue n'était pas mise en œuvre de manière effective puisque, si la durée de conservation prévue par le registre de la RATP était de dix-huit mois à partir de la tenue de la commission de classement pour laquelle ils sont établis, l'autorité a constaté que des fichiers datant de 2017 étaient présents sur certains serveurs.

3. Sur le manquement à la sécurisation des données

L'article 32 du RGPD énonce que le responsable de traitement doit « *mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

En l'espèce, la CNIL a retenu plusieurs manquements à l'article 32 du RGPD en raison de l'absence de différenciation des différents niveaux d'habilitation des agents ayant accès aux données figurant sur l'application utilisée pour le traitement et la gestion des ressources humaines ainsi que les fichiers de préparation des commissions de classement.

4. Sur la sanction

Tirant les conséquences de ces manquements au RGPD, la CNIL a prononcé à l'encontre de la RATP une amende administrative d'un montant de 400.000 euros.

Lien vers la décision :

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044286815?init=true&page=1&query=san-2021-019&searchField=ALL&tab_selection=all

SANCTION D'UNE COMPAGNIE D'ASSURANCE POUR AVOIR ENVOYE DES MAILS AUX MAUVAIS DESTINATAIRES

Par une délibération du 5 aout 2021 la CNPD, autorité de contrôle luxembourgeoise, a prononcé une sanction à l'encontre d'une compagnie d'assurance d'un montant de 135 000 € pour violation de plusieurs principes du RGPD.

L'autorité de contrôle luxembourgeoise a été saisie le 20 mai 2019 d'une plainte d'un client d'une compagnie d'assurance signalant que des courriers électroniques comprenant les données médicales le concernant avaient été envoyés à un destinataire tiers par erreur.

L'autorité de contrôle a effectué un contrôle sur place le 19 juillet 2019, et demandé quelques jours plus tard la fourniture de précisions de la part de l'assureur.

A l'issue de son enquête, l'autorité de contrôle a constaté que la compagnie d'assurance avait commis plusieurs manquements :

(i) Le manquement lié à l'obligation de documenter une violation de données à caractère personnel

Rappelant l'obligation de documenter toute violation de données à caractère personnel (découlant du principe d'accountability des articles 5(2) et 24 du RGPD), l'autorité de contrôle a constaté que le registre des violations de données ne comportait aucune inscription. Estimant que l'envoi de courriers électroniques concernant des données à caractères personnel à un destinataire erroné devait être qualifié de violation de données, le manquement à l'article 33(5) du RGPD était caractérisé.

(ii) Le manquement lié à l'obligation de notifier une violation de données à caractère personnel à l'autorité de contrôle

Selon les dispositions de l'article 33(1) du RGPD, le responsable du traitement est tenu de notifier toute violation de données à caractère personnel à l'autorité de contrôle dans un temps limité. Dès lors que l'envoi de courriers électroniques à un mauvais destinataire a été qualifié de violation de données, l'autorité de contrôle en a logiquement déduit qu'une notification aurait dû être effectuée. En l'absence de cette dernière, le responsable du traitement n'a pas respecté les termes de l'article 33(1) du RGPD.

(iii) Le manquement lié à l'obligation de communiquer à la personne concernée une violation de données à caractère personnel

L'autorité de contrôle a d'abord estimé que les données à caractère personnel impliquées dans le présent cas étaient des données très sensibles concernant la santé du plaignant et dont la divulgation peut entraîner des dommages matériels ou moraux, tels qu'une discrimination, des pertes financières ou des dommages économiques et sociaux importants.

Elle a, dès lors, considéré que la violation présentait un risque élevé pour les droits et libertés du plaignant. Le responsable du traitement se trouvait ainsi dans l'obligation de communiquer à la personne concernée l'ensemble des informations requises en application de l'article 34 du RGPD.

(iv) Le manquement lié à l'obligation de garantir la sécurité des traitements de données à caractère personnel

Conformément aux articles 5(1)f et 32 du RGPD, le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

En l'espèce, l'autorité de contrôle, rappelant que la protection de la confidentialité et de la sécurité des données à caractère personnel constitue un enjeu encore plus important en cas de traitement de données sensibles, a constaté que l'envoi des courriers électroniques litigieux n'était protégé par aucune mesure technique permettant notamment de garantir la confidentialité des messages et documents transmis. L'autorité de contrôle a donc estimé que le responsable du traitement n'a pas respecté ses obligations en matière de sécurité prévues aux articles 5.1.f) et 32.1. a) et b) du RGPD.

Tirant les conséquences de ces manquements au RGPD, l'autorité de contrôle a infligé à la compagnie d'assurance une amende d'un montant de 135.000 € et a enjoint la société de se mettre en conformité dans un délai de 2 mois, tout particulièrement en protégeant l'envoi de courriers électroniques par des mesures de sécurité appropriées, comme le chiffrement, l'utilisation de mots de passe solides ou tout autre technique garantissant une protection similaire.

Lien vers la décision :
https://bit.ly/3Cr5utS

ACTUALITE EUROPEENNE :

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITES NATIONALES DE CONTROLE

Sanction d'un employeur pour avoir contrôlé les heures de travail de ses employés à l'aide d'un système par empreinte digitale

AEPD (ESPAGNE), 26 OCTOBRE 2021

Une entreprise de logistique espagnole a mis en place un système de contrôle des empreintes digitales permettant d'enregistrer les heures de travail de ses salariés.

Plusieurs salariés, estimant que ce système porte atteinte à leurs droits et libertés fondamentaux, ont déposé une plainte auprès de l'autorité de contrôle espagnole.

L'autorité de contrôle a constaté que l'entreprise en question n'avait pas réalisé d'analyse d'impact concernant ce traitement et a, en conséquence, prononcé une amende de 16.000 € à l'encontre de cette dernière.

Lien vers la décision en espagnol : https://bit.ly/3oFAce4

Un club de sport sanctionné pour avoir ajouté une personne sur un groupe WhatsApp sans son consentement

AEPD (ESPAGNE), 5 OCTOBRE 2021

Une ancienne adhérente d'un club de sport, avec lequel elle n'avait plus de lien depuis 10 ans, a été ajoutée sans son consentement sur un groupe de discussion WhatsApp.

La personne concernée a déposé une plainte auprès de l'autorité de contrôle espagnole, qui a ouvert une enquête sur cet incident.

Après avoir rappelé le principe de la limitation de la durée de conservation des données posé à l'article 5 (1) e du RGPD, rappelé la définition de consentement posé à l'article 6 du RGPD et rappelé qu'un responsable du traitement devait mettre en place les mesures de sécurité adéquates en vertu de l'article 32 du RGPD, l'autorité de contrôle a considéré que le club de sport avait traité les données à caractère personnel de la plaignante sans son consentement et en ayant conservé lesdites données au-delà de la durée nécessaire eu égard aux finalités.

En outre, l'autorité de contrôle a estimé que le fait de fournir le numéro de téléphone portable d'une personne à des tiers entraînait une violation de la confidentialité des données personnelles, et donc constituait une infraction à l'obligation de sécurité du traitement.

En conséquence, l'autorité de contrôle a infligé au club de sport une amende de 4.000 €.

Lien vers la décision en espagnol : https://bit.ly/3x3YdPN

L’absence d’utilisation de la fonction copie cachée (cci) peut entraîner des risques pour les droits des individus

ICO (ROYAUME-UNI), 18 OCTOBRE 2021

L’autorité anglaise de contrôle a ouvert une enquête à l’encontre de l’association à but non lucratif HIV Scotland après qu’un email adressé à 105 personnes atteintes du VIH ait été envoyé sur une liste de diffusion visible par tous les destinataires (dont 65 des adresses permettaient une identification des personnes en laissant la possibilité de tirer des conclusions sur l’immunodéficience des personnes).

Au cours de son enquête, l’autorité de contrôle a relevé des lacunes dans les procédures d’envoi de courriers électroniques, et plus précisément une absence de formation adéquate du personnel, une inadéquation de la politique de protection des données et une absence d’utilisation de la méthode de la copie carbone invisible (cci) permettant d’envoyer de manière massive des emails sans divulguer de données personnelles.

Plus encore, l’autorité de contrôle a également constaté que le responsable du traitement avait fait l’acquisition d’un système permettant d’envoyer massivement des messages de manière sécurisée, mais que ce système était inutilisé, et que la méthode de la copie carbone invisible (cci), moins sécurisée, était toujours utilisée.

L’autorité de contrôle a rappelé qu’en vertu des articles 5 (1) f et 32 (1) et (2) du RGPD, les responsables du traitement doivent mettre en place les mesures techniques et organisationnelles appropriées pour garantir la sécurité des données personnelles.

Constatant l’absence de telles mesures, l’autorité de contrôle a infligé à l’organisation à but non lucratif une amende d’un montant de 10 000 £.

Lien vers le communiqué en anglais : https://bit.ly/3DwChPu

Utilisation de brochures directement destinées aux enfants pour fournir une information totalement conforme au RGPD

DATATILSYNET (DANEMARK) 21 SEPTEMBRE 2021

L'autorité de contrôle danoise a ouvert une enquête à l'encontre d'une entreprise réalisant des tests de dépistage au covid 19 sur des enfants en école primaire et au collège.

Dans le cadre de son enquête, l'autorité de contrôle a constaté que l'entreprise disposait d'une politique de confidentialité qui était transmise aux enfants ainsi qu'à leurs responsables légaux via une plateforme de communication numérique utilisée par les écoles et dont l'entreprise encourageait la lecture.

L'autorité de contrôle a, de plus, estimé que la politique de confidentialité contenait toutes les informations nécessaires au sens de l'article 13 du RGPD, et plus généralement qu'aucune violation du RGPD n'était présente.

En revanche, rappelant qu'en vertu de l'article 12 du RGPD l'information doit être fournie « à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant », l'autorité de contrôle a recommandé au responsable du traitement de fournir une information directement destinée aux enfants, en usant de mentions d'informations simplifiées, tant sur la forme que sur le fond.

Lien vers le site en danois : https://bit.ly/30IeM80

ACTUALITE DU CABINET

DERRIENNIC ASSOCIES PROPOSE UN PROGRAMME DE FORMATION DE **35 HEURES** POUR LA PRÉPARATION A LA CERTIFICATION DPO

OBJECTIF

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

COUT

3000€ HT/personne

INTERVENANT

Alexandre FIEVEE
Avocat Associé
Tél : 01.47.03.14.94
afievee@derriennic.com

Classements
Alexandre Fievee figure dans le classement BestLawyers dans la catégorie « Information Technology Law » (2020).
Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie « Next Generation Partners ».

RENSEIGNEMENTS PRATIQUES

Prochaine session 2021/2022 :
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