La Newsletter RGPD par @DerriennicParis

DERRIENNIC ASSOCIÉS

#NewsDerriennicRGPD 27

Madame, Monsieur,

Nous vous invitons, en ce mois de novembre 2020, à voyager au-delà des frontières de l'hexagone et à vous intéresser à deux sanctions particulièrement importantes prononcées par l'autorité de contrôle britannique. Les très attendues recommandations du CEPD sur les « mesures supplémentaires » de l'arrêt Schrems II ont également fait leur apparition et la Commission européenne nous a laissé entrevoir la rédaction qu'elle pourrait adopter, s'agissant de ses nouvelles Clauses Contractuelles Types.

Sommaire

Nous vous proposons donc, de découvrir les articles suivants :

Nous vous en souhaitons une bonne lecture.

Formation à la préparation à 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.

Amende de 18,4 millions de livres pour un accès frauduleux à 339 millions de comptes clients

L'autorité de contrôle britannique en matière de protection des données (« ICO ») a prononcé une amende de plusieurs millions de livres à l'encontre du groupe hôtelier Mariott, à la suite d'une atteinte à l'obligation de sécurité des données.

En 2014, le système de traitement de l'information de la société hôtelière Starwood avait fait l'objet (avant d'être rachetée en 2016 par Mariott) d'une attaque informatique de nature inconnue, qui avait permis à l'attaquant de disposer d'un accès durable aux données à caractère personnel de cette société.

Entre 2016 et 2018, les données à caractère personnel relatives à 339 millions de compte clients Starwood ont fait l'objet d'accès frauduleux.

En 2018, en tentant d'accéder aux données relatives aux cartes bancaires, l'attaquant avait déclenché une alerte, ce qui avait permis à Mariott de prendre connaissance de l'attaque et d'y mettre un terme.

Mariott a notifié l'attaque à l'ICO le 22 novembre 2018, ce qui a déclenché une enquête de l'autorité de contrôle britannique. Cette dernière a, dans cette affaire, endossé le rôle d'autorité chef de file et a soumis son projet de décisions aux autres autorités de contrôle concernées.

Après investigations, l'ICO a reproché à Mariott d'avoir manqué à son obligation de sécurité des données. En particulier, Mariott aurait dû mettre en œuvre des mesures permettant d'identifier les violations de données et de prévenir les accès frauduleux, notamment en

surveillant l'activité des utilisateurs du système d'information.

L'ICO a, en conséquence, par une décision du 30 octobre 2020, décidé de prononcer une amende de 18,4 millions de livres à l'encontre de Mariott.

Les éléments suivants ont été pris en compte dans la détermination du montant de cette amende :

- le nombre particulièrement élevé de personnes concernées ;
- les conséquences de ce manquement sur les personnes concernées, notamment en terme d'anxiété ;
- la durée de l'accès frauduleux ;
- le degré de coopération dont a fait preuve Mariott, le fait qu'elle ait notifié la violation et qu'elle n'ait pas commis de précédent manquement ;
- l'impact de la crise sanitaire liée à la Covid-19 sur Mariott.

Lien vers la publication de la CNIL sur le sujet : https://www.cnil.fr/fr/cybersecurite-ico-en-cooperation-avec-la-cnil-inflige-amendes-record

Lien vers la publication de l'ICO : https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/

British Airways condamnée par l'ICO à une amende de 20 millions de livres

L'autorité de contrôle britannique en matière de protection des données (« ICO ») a prononcé une amende de 20 millions de livres à l'encontre de British Airways à la suite d'une atteinte à son obligation de sécurité des données.

Entre juin et septembre 2018, une application interne de British Airways avait fait l'objet d'une attaque informatique conduite au moyen d'une « accréditation compromise », dont l'objet était d'extraire des données relatives aux cartes bancaires des clients.

L'attaquant avait, en premier lieu, eu accès aux identifiants de connexion de certains prestataires de British Airways. Il avait utilisé ces identifiants afin de se connecter à l'outil de connexion à distance de British Airways, puis avait obtenu, via une faille connue de British Airways, accès à un fichier contenant le nom d'utilisateur et le mot de passe d'un compte administrateur.

L'attaquant avait utilisé de ces données pour se connecter à différents serveurs et extraire un certain nombre de données à caractère personnel, y compris des numéros de cartes bancaires.

British Airways a été mise au fait de cette attaque, qui concernait 429 612 personnes, par un tiers, et a corrigé la vulnérabilité quelques minutes après avoir été prévenue. Cette attaque a rapidement été portée à la connaissance de l'ICO par British Airways.

L'ICO, au terme de son enquête, a relevé que British Airways aurait pu mettre en œuvre un certain nombre de mesures de nature à assurer la sécurité des données, dont les mesures suivantes :

- sécuriser le fichier contenant les identifiants de connexion de son prestataire ;
- ne pas permettre aux tiers d'accéder au système de traitement de l'information au moyen d'une authentification à un seul facteur ;
- ne pas permettre l'accès au moyen d'un mot de passe administrateur codé en dur ;
- surveiller l'accès aux fichiers pertinents.

L'ICO a affirmé que le niveau de complexité de cette attaque n'était pas de nature à exonérer British Airways de sa responsabilité.

Compte tenu de ces manquements à l'obligation de sécurité des données, l'ICO a décidé de prononcer à l'encontre de British Airways une amende d'un montant de 20 millions de livres, au regard des éléments suivants :

- il n'est pas certain que British Airways aurait pu prendre connaissance de la violation sans l'intervention du tiers ;
- les données en cause comprennent des cartes bancaires en grand volume, ce qui rend la violation particulièrement inquiétante ;
- British Airways a immédiatement pris des mesures afin de réduire le dommage subi par les personnes concernées, les a rapidement informées, ainsi que l'ICO ;
- l'attaque a affecté l'image de marque de British Airways, ce qui a eu un effet dissuasif sur cette dernière, ainsi que sur les autres responsables du traitement ;

- British Airways a proposé aux personnes concernées par l'attaque de leur rembourser les sommes qui auraient pu leur être volées à la suite de l'attaque ;
- la pandémie liée à la Covid-19 a eu des conséquences négatives sur les revenus de British Airways.

Lien vers la publication de la CNIL sur le sujet : https://www.cnil.fr/fr/cybersecurite-ico-en-cooperation-avec-la-cnil-inflige-amendes-record

Lien vers la publication de l'ICO : https://ico.org.uk/action-weve-taken/enforcement/british-airways/

Les recommandations du CEPD sur les « mesures supplémentaires » évoquées par l'arrêt Schrems II

Le Comité européen de la Protection des données (« CEPD ») a publié, le 10 novembre 2020, un document dans lequel il formule des recommandations quant aux « mesures supplémentaires » aux outils de transfert de données hors UE permettant d'assurer un niveau de protection des données équivalent à celui de l'Union européenne.

Pour rappel, la Cour de justice de l'Union européenne (CJUE) a, par une décision du 16 juillet 2020, estimé que les exportateurs de données à caractère personnel doivent s'assurer, au cas par cas, que les lois et pratiques des pays tiers à l'UE (destinataires des données) n'entravent pas l'efficacité des garanties appropriées (Clauses contractuelles types, etc.) permettant le transfert de donnes à caractère personnel vers ces pays (voir notre article). Dans le cas où ces lois et pratiques entravent l'efficacité des telles garanties, les exportateurs de données doivent mettre en œuvre des « *mesures supplémentaires* » afin de combler les lacunes des lois et pratiques du pays de destination des données.

Afin d'aider les exportateurs de données dans leur travail (i) d'évaluation du niveau de protection offert par les pays tiers et (ii) d'identification des « mesures supplémentaires » appropriées, le CEPD a adopté, le 10 novembre 2020, plusieurs recommandations.

I. S'agissant de l'évaluation du niveau de protection offert par le pays tiers destinataire des données, elle doit se concentrer sur la législation applicable au transfert et à l'outil de transfert dont elle peut entraver l'efficacité.

Le CEPD invite, à ce titre, à se référer à son guide du 13 avril 2016 intitulé « *European Essential Guarantees recommendations* » qui avait pour objet de traiter des conséquences de l'invalidation du Safe Harbor.

Cette évaluation du niveau de protection doit être particulièrement méticuleuse lorsque la législation applicable est ambiguë ou bien n'est pas accessible au public.

En l'absence de législation applicable, l'exportateur doit être attentif aux facteurs objectifs pertinents, et ne pas se reposer sur des facteurs subjectifs, tels que la vraisemblance d'un accès de la part des autorités publiques non-adéquat aux standards européens.

Ce travail d'évaluation doit être mené avec diligence, être documenté et être renouvelé à « *intervalles appropriés* ».

Si cette évaluation révèle que les lois et/ou pratiques sont susceptibles d'entraver les garanties appropriées, l'exportateur doit identifier et adopter les « *mesures supplémentaires* » permettant de porter le niveau de protection des données transférées à un niveau équivalent à celui des standards européens.

II. S'agissant des « *mesures supplémentaires* », le CEPD en fournit une liste non-exhaustive :

- appliquer un chiffrement conforme à l'état de l'art avant de transférer les données, sans que le destinataire ne dispose d'une clé de déchiffrement, à moins que ce destinataire ne soit protégé par les lois du pays tiers (par exemple, par un secret professionnel) ;

- pseudonymiser les données avant leur transfert ;

- s'assurer que les données sont traitées par plusieurs sous-traitants indépendants situés dans différentes juridictions, sans que le contenu des données ne leur soit communiqué ; avant leur transmission, les données doivent être divisées de telle sorte que les données adressées à l'un des sous-traitant ne permet pas de « reconstruire » tout ou partie des données à caractère personnel.

Le CEPD indique n'avoir pas identifié de « *mesure supplémentaire* » dans les cas suivants :

- un transfert de données vers un prestataire « Cloud », dont le service nécessite un accès aux données en clair, situé dans un pays dont les autorités ont un pouvoir d'accès aux données qui va au-delà de ce qui est nécessaire dans une société démocratique ;

- un accès en clair aux données personnelles de l'exportateur, par un responsable du traitement situé dans un pays tiers à l'EEA, dont les autorités ont un pouvoir d'accès aux données qui va au-delà de ce qui est nécessaire dans une société démocratique.

Dans ces deux situations, le CEPD considère que le chiffrement des données ne saurait constituer une « *mesure supplémentaire* », si le destinataire des données est en possession d'une clé de déchiffrement.

Dans ce contexte, nous vous invitons à vous référer à nos recommandations.

Lien vers les recommandations du CEPD : https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

La Commission européenne publie deux projets de « Clauses Contractuelles Types »

Le 12 novembre dernier, la Commission européenne a publié deux projets de décisions d'adoption de « Clauses Contractuelles Types » (« CCT »). L'un applicable aux transferts de données vers des pays tiers à l'Union européenne (« UE »), l'autre aux relations entre un responsable du traitement et un sous-traitant situés au sein de l'UE.

Jusqu'à présent, les CCT avaient pour objet d'encadrer les transferts de données personnelles vers des pays tiers à l'UE, soit de responsable du traitement à responsable du traitement, soit de responsable du traitement à sous-traitant.

La Commission européenne, qui n'avait pas actualisé ses CCT depuis l'entrée en vigueur du RGPD, a, le 12 novembre dernier, publié un projet de CCT applicable dans le cadre d'un transfert de données personnelles en dehors de l'UE entre plusieurs organismes. Par ailleurs, elle propose un projet de CCT ayant pour objet d'encadrer les relations entre un responsable du traitement et un sous-traitant, indépendamment de l'existence d'un transfert de données personnelles hors UE.

1. S'agissant des CCT pour les transferts vers des pays tiers à l'UE

Le projet publié par la Commission européenne (accessible ici) a pour objectif de remanier les CCT jusqu'alors utilisées pour encadrer les transferts de données personnelles en dehors de l'UE, à la lumière de la décision de la CJUE le 16 juillet dernier « Schrems II » (la décision est accessible ici et notre résumé ici).

La publication de ce projet intervient deux jours après la publication des recommandations du Comité européen à la protection des données (« CEPD ») relatives aux mesures supplémentaires devant être mises en œuvre dans le cadre de ces transferts (les recommandations sont accessibles ici et notre résumé ici).

Les principaux apports de ce projet sont :

- L'encadrement dans un document unique, des transferts :
  - De responsable du traitement à responsable du traitement ;
  - De responsable du traitement à sous-traitant ;
  - De sous-traitant à sous-traitant ;
  - De sous-traitant à responsable du traitement.
- Une clause (indiquée comme « optionnelle ») permettant aux CCT d'évoluer au cours de leur exécution en offrant aux tiers, la possibilité d'adhérer aux CCT, à tout moment, sous réserve de l'accord des parties.
- Des clauses spécifiques pour répondre aux préoccupations soulevées par la décision de la CJUE « Schrems II », telles que :
  - L'obligation d'évaluer si les CCT permettent de garantir un niveau de protection équivalent à celui du RGPD en tenant compte (i) des lois nationales du pays tiers, (ii) des « circonstances particulières du transfert » et, (iii) des garanties supplémentaires mises en œuvre (telles que des mesures techniques ou organisationnelles) et, de documenter cette évaluation.
  - Des obligations spécifiques aux importateurs de données en cas de tentatives des autorités publiques

de son pays d'accéder à des données personnelles provenant de l'UE comme notamment, (i) l'obligation pour l'importateur d'informer, dans la mesure du possible, l'exportateur de données et la personne concernée qu'il a reçu une demande d'accès à ces données de la part d'une autorité publique ; (ii) l'obligation d'évaluer la légalité de la demande au regard du droit national et, le cas échéant, de contester cette demande ; et (iii) l'obligation de divulguer le minimum de données personnelles, raisonnablement possible, à l'autorité publique.

Le projet de décision d'adoption des CCT prévoit que les organismes qui utilisent actuellement des CCT pour garantir le transfert de données personnelles en dehors de l'UE, auront un délai d'un an pour mettre en place les nouvelles clauses.

2. **S'agissant des CCT entre responsables du traitement et sous-traitants situés dans l'UE**

Parallèlement, la Commission européenne a publié un projet de décision d'adoption de CCT (accessible ici) pouvant être utilisé pour encadrer les relations entre un responsable du traitement un sous-traitant, situés dans l'UE.

Ce projet comporte des clauses permettant de satisfaire aux exigences imposées par l'article 28 du RGPD, notamment relatives à la détermination des caractéristiques des traitements opérés par le sous-traitant pour le compte du responsable du traitement, aux mesures de sécurité mises en œuvre, au recours à la sous-traitance ultérieure, au transfert des données personnelles en dehors de l'UE, etc.

Le projet de décision d'adoption des CCT prévoit que l'utilisation de ces clauses ne sera pas obligatoire.

Ces documents sont soumis à consultation jusqu'au 10 décembre 2020.

Envoi de courriers de félicitations aux bacheliers : la CNIL rappelle à l'ordre un rectorat et une députée

Le rectorat de l'académie de Normandie, ainsi qu'une députée, ont fait l'objet d'un rappel à l'ordre de la CNIL dans le cadre d'un échange de données à caractère personnel visant à féliciter des bacheliers.

La CNIL a été saisie d'une plainte concernant l'envoi, par une députée, de courriers de félicitations aux lauréats du baccalauréat 2019.

Après avoir été interrogée par la CNIL sur les faits qui lui étaient rapportés, la députée a affirmé que son équipe avait été rendue destinataire, à sa demande, d'un fichier émanant du rectorat de l'académie de Normandie, comportant les coordonnées des lauréats du baccalauréat du département. Elle a expliqué que son équipe avait traité les nom, prénom, et adresse postale de ces lauréats aux fins de publipostage, et avait ensuite détruit le fichier.

Les investigations menées par la CNIL ont révélé que les données étaient issues du traitement « OCEAN », relatif à la gestion des examens et concours scolaires, créé par un arrêté de 2013.

La CNIL, qui souligne que cet arrêté ne listait pas les parlementaires comme personnes habilitées à être destinataires des données issues du traitement OCEAN, a considéré que la députée ne pouvait donc pas être rendue destinataire de ces données, et n'était pas habilitée à opérer un traitement distinct, en son nom et pour son compte, des données. Le rectorat, pour sa part, ne pouvait pas procéder à un transfert de données à caractère personnel à une personne ne figurant pas sur la liste des personnes autorisées à accéder aux données.

Tant la députée, que le rectorat, ont, en conséquence, méconnu les termes de l'arrêté de 2013 et, partant, ont procédé à un traitement illicite des données.

La CNIL a, par ailleurs, relevé un certain nombre d'éléments aggravants :

- le nombre élevé de personnes concernées ;
- le caractère sensible du public affecté, composé en grande partie de mineurs ;
- concernant la députée, le fait qu'elle exerce des fonctions publiques, dont la qualité d'élue suscite des attentes légitimes en termes de légalité et de rigueur ;
- concernant le rectorat :
    - le fait que les données ont été envoyées à la députée dans des conditions non sécurisées, à savoir l'envoi d'un fichier Excel en pièce jointe non chiffrée d'un courriel ;
    - le fait que la demande de la députée n'a pas fait l'objet d'une analyse par les services du rectorat, et n'a pas été transmise au DPO pour avis ;
    - le fait que la transmission a eu lieu sans aucune forme de contrôle *a priori* et sans autre forme de contrôle *a posteriori*, quant à l'utilisation et la suppression des données personnelles par les équipes de la députée, que la demande de production d'une attestation sur l'honneur de destruction du fichier.

La CNIL a, en conséquence, prononcé un rappel à l'ordre à l'encontre de la députée et du rectorat.

Lien vers les décisions de la CNIL :

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042348000?tab_selection=all&searchField=ALL&query=SAN-2020-005&searchType=ALL&typePagination=DEFAULT&pageSize=10&page=1#all

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042348029?tab_selection=all&searchField=ALL&query=SAN-2020-006&searchType=ALL&typePagination=DEFAULT&pageSize=10&page=1#all

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

COÛT

3000€ HT/personne

INTERVENANT

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

CLASSEMENTS

Alexandre Fievee figure dans le classement Best Lawyers 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 2020/2021 :
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