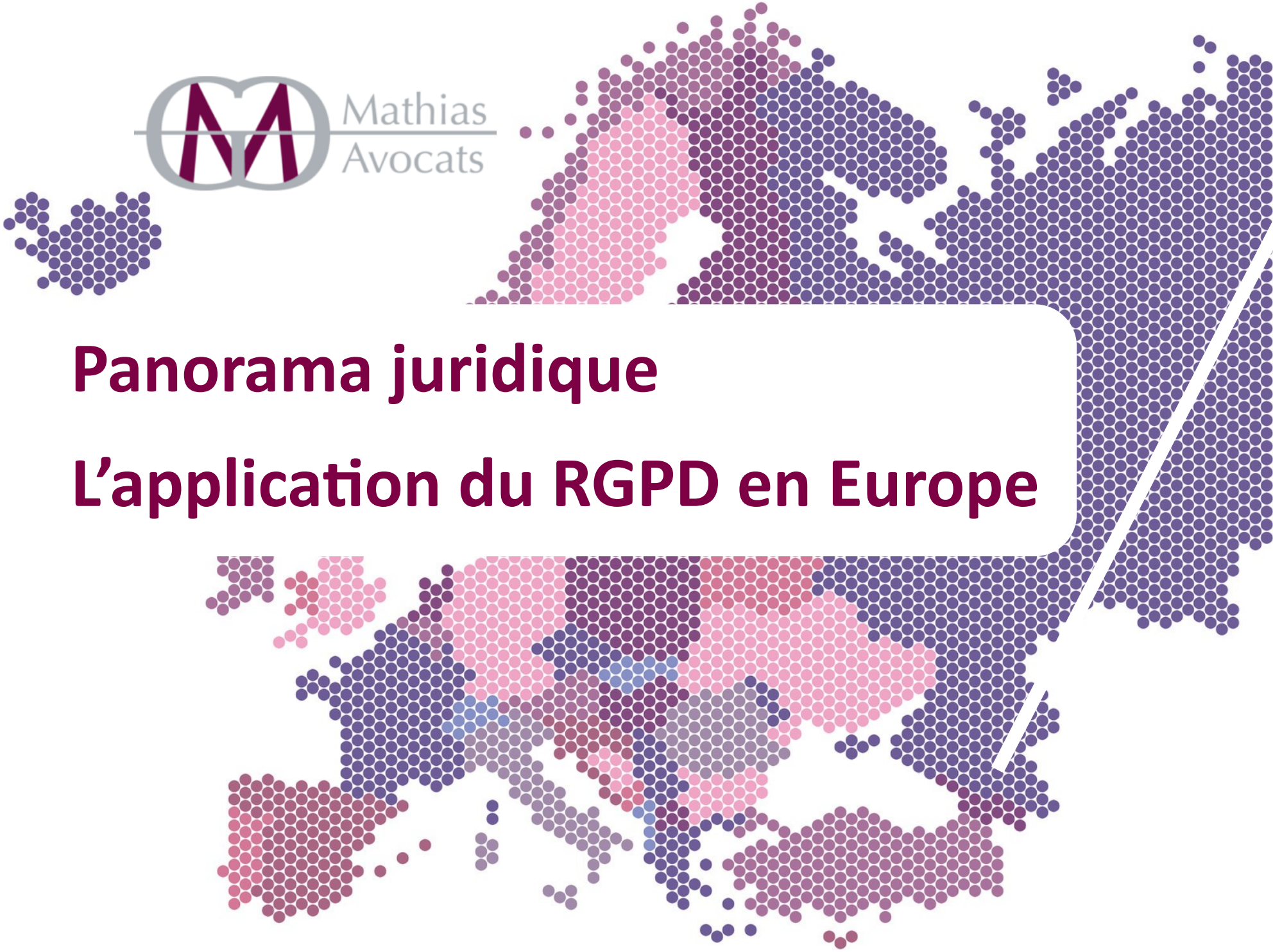
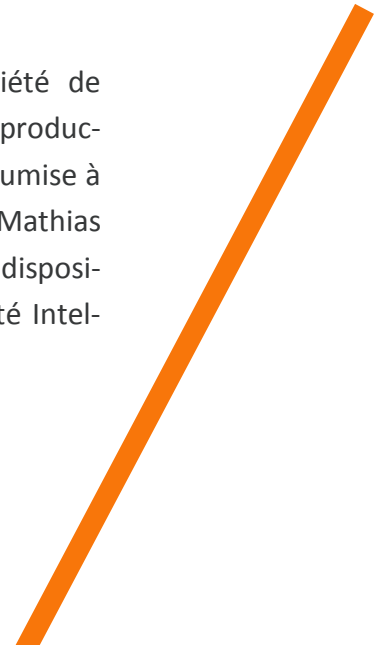
Mathias Avocats

Panorama juridique

L'application du RGPD en Europe





SOMMAIRE

INTRODUCTION

Une année s'est écoulée depuis l'entrée en application du Règlement général sur la protection des données (RGPD). Ce cadre de protection des données, unique au monde, a permis d'unifier les pratiques sur le territoire de l'Union européenne. Cependant, cette harmonisation passe également par la « jurisprudence » des diverses autorités de contrôle chargées de faire respecter ce texte.

C'est pourquoi il nous paraissait essentiel de vous présenter les différentes décisions et sanctions prononcées depuis le 25 mai 2018.

À ce sujet, le Comité européen de la protection des données (CEPD) a publié un bilan sur le RGPD. Ainsi, nous apprenons que les autorités de contrôle auraient traité environ 206 300 dossiers entre le 25 mai 2018 et fin février 2019 (94 622 dossiers à la suite d'une plainte et 64 684 dossiers à la suite d'une notification de violation de données). Le CEPD précise également que 11 autorités de contrôle ont prononcé des sanctions pécuniaires, pour un montant total de presque 56 000 000 d'euros.

Pour le premier anniversaire du RGPD, Mathias Avocats a souhaité publier ce panorama afin d'illustrer la diversité des mesures prises par les autorités de contrôle et des manquements identifiés par celles-ci.

Vous pourrez notamment y retrouver les critères pris en compte par les autorités pour déterminer la sanction prononcée. Par ailleurs, le caractère récurrent de certains manquements vous oriente dans vos démarches de mise en conformité. D'expérience, la connaissance de la « jurisprudence » enrichit la pratique ; qu'il s'agisse de mettre en conformité une entité ou de la défendre dans le cadre d'une procédure de contrôle.

Nous vous souhaitons ainsi une bonne lecture, en espérant que ce panorama vous sera utile dans vos projets.

Dans l'attente de partager notre expertise avec vous,

Bien cordialement,

Garance Mathias

Avocat Associée

ALLEMAGNE

Il existe seize autorités de contrôle locales (une par *Länder*) en Allemagne. La cohérence entre les positions de ces autorités est assurée par une entité nationale (*Datenschutzkonferenz*) composée d'un représentant de chacune des autorités de contrôle. La représentation de l'Allemagne auprès du Comité européen sur la protection des données (CEPD) est quant à elle assurée par le Préposé fédéral à la protection des données et à la liberté de l'information (*Bundesbeauftragte für Datenschutz und Informationsfreiheit*), autorité fédérale compétente dans le secteur des télécommunications.

L'Allemagne a adopté le 5 juillet 2017 une loi adaptant le droit allemand au RGPD (*Bundesdatenschutzgesetz*), entrée en application le 25 mai 2018.

A la page suivante, vous trouverez le résumé d'une décision prononçant une sanction pécuniaire de 20 000 euros prononcée à l'encontre d'un réseau social, pour manquement à son obligation d'assurer la sécurité des données.

Autorité de contrôle	Décision	Date	Manquements relevés	Faits reprochés
Autorité de Baden-Württemberg	Sanction pécuniaire de 20 000 €	21 novembre 2018	Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité des données (*article 32, 1 du RGPD*)	Un réseau social a fait l'objet d'une cyberattaque en septembre 2018. A la suite de la violation, la société a notifié les personnes concernées et l'autorité de contrôle dans les délais qui lui étaient impartis. Toutefois, il a été relevé que les mots de passe des utilisateurs étaient conservés en clair dans la base de données de la société, qui a été copiée par les attaquants. Pour l'autorité, il s'agit d'une non-conformité à l'obligation du réseau social de définir des mesures de sécurité adéquates au regard des risques. L'autorité a toutefois déclaré avoir pris en compte la « *coopération exemplaire* » dont a fait preuve la société dans la détermination du montant de la sanction pécuniaire. En effet, la société a été transparente vis-à-vis de l'autorité de contrôle et des personnes concernées, réactive, et a rapidement effectué des investissements financiers importants pour implémenter les correctifs de sécurité nécessaires.

AUTRICHE

En Autriche, l'autorité de contrôle est appellée *Österreichische Datenschutzbehörde* ou DSB. Elle est chargée du contrôle du respect du RGPD et des diverses lois nationales relatives à la protection des données adoptées par l'Autriche dont la principale, la loi sur la protection des données (*Datenschutzgesetz*) qui a été modifiée en 2018.

Dans les pages suivantes, vous trouverez la synthèse de deux décisions prononcées par cette autorité.

La première est une sanction pécuniaire de 4 800 euros à l'encontre du gérant d'un commerce pour la mise en place d'un dispositif de vidéosurveillance non conforme à la règlementation.

Dans la seconde, l'autorité a ordonné à la Poste autrichienne de cesser un traitement et de supprimer les données correspondantes en raison de plusieurs manquements.

Décision	Date	Manquements relevés	Faits reprochés
Arrêt du traitement Suppression des données collectées	Février 2019	• Manquement à l'obligation de disposer d'une base légale (*article 5,1,a et article 6 du RGPD*) • Traitement de données sensibles sans recueil du consentement ou d'autre base légale (*article 9, 2 du RGPD*) • Analyse d'impact réalisée de manière incorrecte (*article 35 du RGPD*) • Registre des activités de traitement incorrectement tenu (*article 30 du RGPD*)	A l'issue d'un contrôle, l'autorité de contrôle autrichienne a constaté que la Poste (Österreichische Post) avait violé plusieurs dispositions du RGPD. En effet, la Poste traitait des données sensibles et, plus particulièrement, déterminait les préférences politiques des personnes physiques au moyen de méthodes statistiques. L'autorité a constaté que ce traitement était mis en œuvre en l'absence de consentement explicite des personnes concernées et de toute autre base légale. Par ailleurs, l'analyse d'impact réalisée par la Poste était erronée. Par conséquent, l'autorité a ordonné à la Poste de cesser le traitement, de supprimer les données collectées et de réaliser une nouvelle analyse d'impact pour rectifier son registre des activités de traitements.
Sanction pécuniaire de 4 800 euros	Octobre 2018	• Manquement à l'obligation d'information (*articles 12 et 13 du RGPD*) et au principe de transparence (*article 5, 1 a du RGPD*) • Vidéosurveillance illégale	Le gérant d'une boutique avait installé une caméra de vidéosurveillance devant son local. Ce dispositif permettait cependant de capter des images de passants sur le trottoir. Les règles relatives à la vidéosurveillance n'auraient pas été respectées par le responsable du traitement. Notamment, celui-ci n'aurait pas suffisamment informé les personnes concernées de la présence de la caméra et du traitement mis en œuvre. Le faible montant de la sanction est expliqué par l'autorité de contrôle comme une application du principe de proportionnalité des sanctions.

CHYPRE

Pour réviser sa législation antérieure, Chypre a adopté une loi sur la protection des données, entrée en vigueur le 31 juillet 2018. Cette loi prévoit des obligations à la charge de l'autorité de protection des données (*Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*) qui s'ajoutent à celles prévues par le RGPD. Par exemple, l'autorité doit examiner les plaintes des personnes dans un délai de 30 jours à compter de leur réception.

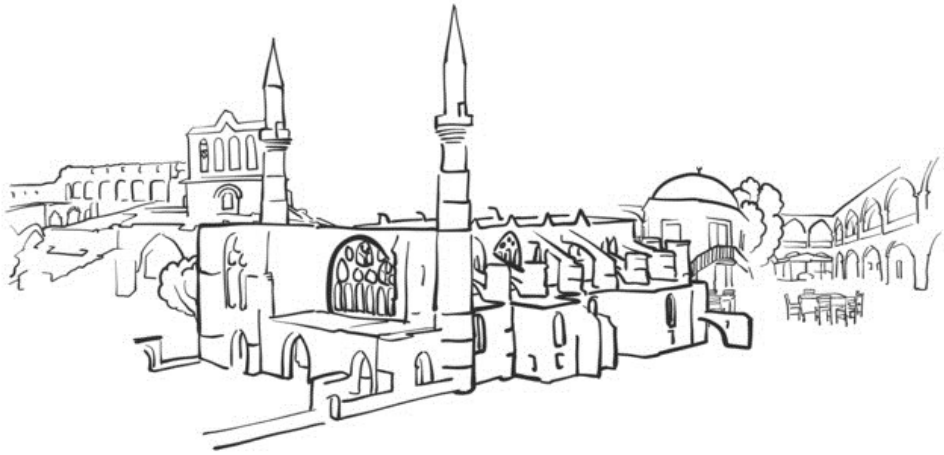
Dans les pages suivantes, vous trouverez les résumés de quatre décisions rendues par cette autorité :

⇒ Une sanction pécuniaire de 10 000 euros à l'encontre d'un journal pour manquements aux principes de licéité du traitement et de minimisation des données ;

⇒ Une sanction pécuniaire de 5 000 euros à l'encontre d'un hôpital pour manquement à son obligation de s'assurer de l'intégralité des données ;

⇒ Un avertissement à l'encontre d'un médecin pour « données mal anonymisées » ;

⇒ Un avertissement à l'encontre de la maire d'une commune pour manquement à son obligation de recueillir le consentement de la personne concernée à la divulgation de ses données.



NICOSIA

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire de 10 000 €	9 janvier 2019	• Manquement au principe de minimisation des données (*article 5, 1, c) du RGPD*) • Manquement au principe de licéité du traitement, faute de base légale déterminée (*article 6 du RGPD*)	Une plainte a été déposée par deux policiers contre le journal « Politis » en raison de la publication de leurs noms et photographies dans un article du 17 juin 2018 portant sur une affaire judiciaire dans laquelle ces policiers étaient impliqués. Le 9 janvier 2019, une sanction pécuniaire de 10 000 euros a été prononcée à l'encontre de ce journal pour avoir manqué à ses obligations en vertu de l'article 5 §1 c) et de l'article 6 du RGPD. Le Commissaire à la protection des données a estimé que l'objectif recherché par le journal aurait pu être atteint en se référant uniquement aux initiales de leurs noms et en floutant leurs visages dans les photos de sorte qu'il ne soit pas possible de les reconnaitre. De plus, le journal n'identifiait pas de base légale pour le traitement en cause. Le journal Politis a formé un recours devant le tribunal administratif contre la déci-
Sanction pécuniaire de 5 000 €	7 novembre 2018	Manquement à l'obligation d'assurer l'intégrité des données (*article 32 du RGPD*) (Perte accidentelle de données à caractère personnel)	Un patient a déposé une plainte auprès du Commissaire à la protection des données parce que sa demande d'exercice du droit d'accès aux données le concernant n'avait pas été satisfaite par un hôpital. Ce dernier n'avait pas pu trouver le fichier contenant les données du patient. Le Commissaire a infligé une amende de 5 000 € à l'hôpital pour perte du fichier. Pour limiter le montant de l'amende, le Commissaire a pris en compte les mesures prises par l'hôpital pour améliorer la situation.

Décision	Date	Manquements relevés	Faits reprochés
Avertissement	14 janvier 2019	Donnée « mal anonymisée » (*article 4,1 du RGPD*) (donnée toujours identifiante)	Un médecin a utilisé une photo du visage de l'un de ses patients lors d'une émission télévisée sur la santé. Afin de dissimuler son identité, il avait apposé une rayure noire sur les yeux de son patient. Ce dernier estimant qu'il était reconnaissable sur la photo, a déposé une plainte auprès du Commissaire. Le 14 janvier 2019, le Commissaire a prononcé un avertissement à l'encontre du médecin en lui rappelant d'être vigilant et de mieux dissimuler l'identité de ses patients à l'avenir.
Avertissement	31 janvier 2019	Manquement à l'obligation de recueillir le consentement (*article 6, 1, a) du RGPD*)	La mairie d'une commune tentait de contacter une personne afin de l'avertir de possibles poursuites dues à ses dettes fiscales, mais n'arrivait pas à la joindre. Lorsque le père de la personne en question a décroché, l'employé de la mairie l'a informé de l'objet de son appel. La personne a saisi l'autorité de contrôle d'une plainte en indiquant que la mairie avait communiqué des données à caractère personnel la concernant à un tiers sans son accord, en l'espèce son père. L'autorité de contrôle estime que la divulgation à une tierce partie des données à caractère personnel n'aurait dû être effectuée qu'après le recueil du consentement de la personne concernée. Au regard des faits et des mesures de sensibilisation mises en œuvre par la municipalité, l'autorité de contrôle ne prononce qu'un avertissement.

DANEMARK

Au Danemark, l'autorité de protection des données (*Datatilsynet)* n'a pas la compétence d'infliger directement une amende. Elle doit établir un rapport, qui sera étudié par les forces de police afin de déterminer s'il existe des motifs suffisants pour engager des poursuites. La sanction est ensuite prononcée par la juridiction compétente.

Le Parlement danois a adopté le 17 mai 2018 une loi sur la protection des données (Databeskyttelsesloven) adaptant le droit national au RGPD. Cette loi est entrée en vigueur le 25 mai 2018. Rappelons qu'elle ne s'applique pas sur le territoire de Groenland et des Îles Féroé.

A la page suivante, vous trouverez le résumé d'une décision prononçant une sanction pécuniaire d'environ 160 630 euros à l'encontre d'une compagnie de taxis, pour manquement aux principes de minimisation des données et de limitation de la durée de conservation.

COPENHAGEN

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire de DKK 1,2M / environ 160 630 euros (À confirmer par la juridiction compétente)	Mars 2019	Manquements aux principes de minimisation des données et de limitation de la durée de conservation (*article 5,1 du RGPD*)	A la suite d'une enquête effectuée en octobre 2018, l'Autorité danoise de protection des données a recommandé une amende de 1,2 millions de couronnes danoises, soit environ 160 630 euros, à l'encontre de la compagnie de taxis « Taxa 4x35 » pour violation du RGPD. En effet, la société déclarait « anonymiser » les données qu'elle collectait sur ses clients au bout de deux ans, mais se contentait de supprimer leurs noms et prénoms. Elle conservait de nombreuses données telles que leurs données de géolocalisation, ou leur numéro de téléphone. Ces derniers étaient conservés pendant trois ans à compter de « l'anonymisation ». De plus, la société n'était pas en mesure de démontrer qu'elle supprimait les données dans les délais énoncés, faute notamment d'une traçabilité complète et de mécanismes de purge automatisée.

FINLANDE

En Finlande, l'autorité chargée de veiller au respect du RGPD et des lois nationales relatives à la protection des données est appelée *Tietosuojavaltuutetun toimisto.*

La Finlande a adopté une loi (*Tietosuojalaki)* adaptant le droit finlandais au RGPD, entrée en vigueur le 1er janvier 2018. Il existe d'autres lois finlandaises relatives à la protection des données, notamment la loi sur les services de communication électroniques (*Laki sähköisen viestinnän palveluista*) et la loi sur la vie privée au travail (Laki yksityisyyden suojasta työelämässä).

A la page suivante, vous trouverez le résumé d'une décision prononçant une mise en demeure à l'encontre d'un établissement de crédit, pour plusieurs manquements notamment au regard de la mise en place d'une décision entièrement automatisée.

Décision	Date	Manquements relevés	Faits reprochés
Mise en demeure	Mars/Avril 2019	Manquements aux obligations de transparence et d'information des personnes concernée, spécifiquement au regard de la mise en place d'une décision entièrement automatisée (*article 13,2,f) ou 14,2,g du RGPD*)	Un établissement de crédit a été mis en demeure par l'autorité de contrôle de mettre en conformité son traitement comprenant une décision entièrement automatisée. Celle-ci servait à évaluer la solvabilité de demandeurs de prêt et relevait de l'article 22, 2) a° du RGPD. Au regard de la loi nationale, l'autorité de contrôle a estimé que certains des critères pris en compte, en particulier l'âge des demandeurs, ne pouvaient servir de base à la prise de décision automatisée. De plus, l'autorité de contrôle finlandaise a estimé que le responsable du traitement ne remplissait pas son obligation d'information, faute de fournir suffisamment d'informations sur la logique sous-jacente à la décision automatisée, son rôle dans la décision d'accorder ou non un crédit et ses conséquences pour le demandeur. L'établissement de crédit avait jusqu'au 30 avril 2019 pour se mettre en conformité.

FRANCE

En France, l'autorité de contrôle chargée de s'assurer du respect du RGPD et du droit national en matière de protection des données est la Commission nationale de l'informatique et des libertés (Cnil).

Avant l'entrée en application du RGPD, la protection des données à caractère personnel était encadrée par la loi Informatique et Libertés. Pour l'adapter au RGPD, elle a été modifiée par la loi du 20 juin 2018 relative à la protection des données et l'ordonnance du 12 décembre 2018 prise en application de cette dernière.

Dans la page suivante, vous trouverez la synthèse d'une décision prononçant une sanction pécuniaire de 50 millions d'euros à l'encontre de la société Google LLC pour manquement à ses obligations de transparence, d'information et de disposer une base légale du traitement faute de consentement valablement recueilli.

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire de 50 millions d'euros	21 janvier 2019	• Violation du principe de transparence (*article 5, 1 a du RGPD*) et manquement à l'obligation d'information (*articles 12 et 13 du RGPD*) • Manquement à l'obligation de disposer d'une base légale pour le traitement (*article 5, 1 a du RGPD*) faute de consentement valablement recueilli (*article 4, 11 et article 7 du RGPD*)	La société Google LLC a fait l'objet de deux plaintes collectives déposées par des associations. A la suite de ces plaintes, la Cnil a diligenté une procédure de contrôle, portant principalement sur les traitements dont font l'objet les données d'une personne créant un compte Google lors du paramétrage d'un téléphone sous le système d'exploitation Android. Concernant l'obligation d'information, il est reproché à la société de délivrer une information qui ne satisfait pas aux objectifs du RGPD en termes de concision, de clarté et de facilité d'accès. Ceci est notamment dû au choix de la société Google LLC de communiquer l'information complète relative au traitement au sein d'une politique de confidentialité portant sur l'ensemble des traitements liés aux services proposés par la société. Le manquement à l'obligation de disposer d'une base légale porte plus précisément sur les traitements liées à la personnalisation des publicités opérées par la société. Celle-ci se fonde sur le consentement (article 6, 1 a), mais la formation restreinte de la Cnil estime qu'elle ne recueille pas réellement le consentement des personnes concernées, faute pour celui-ci d'être libre, spécifique, éclairé et univoque.

GRECE

En Grèce, l'autorité chargée de veiller au respect du RGPD est l'Autorité hellénique de protection des données (*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα).* A ce jour, la loi adaptant le droit national au RGPD n'est pas encore entrée en vigueur. Toutefois, puisqu'il s'agit d'un texte directement applicable sur le territoire de l'Union, l'Autorité hellénique peut se fonder sur le RGPD pour prononcer des mesures correctrices ou des sanctions.

Dans les pages suivantes, vous trouverez le résumé de trois décisions prises par l'autorité grecque :

⇒ Un avertissement prononcé à l'encontre d'une société pour violation du principe de licéité du traitement ;

⇒ Un avertissement prononcé à l'encontre d'un groupe de sociétés en raison des mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement et pour manquement à l'obligation de s'assurer de l'intégrité et de la confidentialité des données ;

⇒ Un avertissement prononcé à l'encontre d'un établissement bancaire pour manquement à son obligation de notification en cas de violation de données.

Décision	Date	Manquements relevés	Faits reprochés
Avertissement	9 novembre 2018	Non-respect du principe de licéité du traitement (*article 5, 1 et article 6,1 a du RGPD*)	Une personne recevait des messages via l'application Viber de la part d'une société la remerciant pour son consentement et déclarant qu'elle continuerait à l'informer des offres spéciales et des événements. La personne a déposé une plainte auprès de l'autorité de contrôle en faisant valoir qu'elle n'avait pas donné son consentement à la collecte de son numéro ni à l'envoi des messages promotionnels. Il ressort des éléments de preuve que la personne concernée avait donné son numéro de téléphone à la société lors d'une transaction effectuée antérieurement. Toutefois, elle n'avait pas consenti à son utilisation pour d'autres finalités et en particulier pour la promotion de produits et de services de la société. Par conséquent, l'autorité de contrôle a prononcé un avertissement à l'encontre
Avertissement	9 novembre 2018	• Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement (*article 32 du RGPD*) • Manquement à l'obligation de s'assurer de l'intégrité et de la confidentialité des données (*article 5,1, f du RGPD*)	Un groupe de sociétés (Dimera) a été la cible d'une attaque informatique affectant la confidentialité des données à caractère personnel qu'il collecte et traite. Le groupe a informé l'autorité de contrôle et les personnes concernées de la violation de données dans les délais après en avoir eu connaissance. Toutefois, l'autorité de contrôle a constaté qu'il n'avait pas mis en œuvre les mesures techniques et organisationnelles permettant de garantir la sécurité du traitement. Elle a prononcé un avertissement à l'encontre du groupe Dimera notamment pour défaut d'installation de mises à jour du logiciel utilisé en matière de sécurité, défaut de mise en place de mécanismes adéquats pour la détection des attaques de sécurité, et défaut de procédures visant à évaluer régulièrement les mesures de sécurité.

Décision	Date	Manquements relevés	Faits reprochés
Avertissement	9 novembre 2018	Manquement à l'obligation de notification d'une violation de données à l'autorité de contrôle (*article 33 du RGPD*) et aux personnes concernées (*article 34 du RGPD*) dans les délais	Un établissement bancaire a communiqué par erreur les données à caractère personnel de certains de ses clients à d'autres. Il a notifié la violation de données à l'autorité de contrôle et aux personnes concernées cinq jours après en avoir eu connaissance. Par conséquent, l'autorité de contrôle a prononcé un avertissement à l'encontre celui-ci pour ne pas avoir signalé la violation de données à caractère personnel dans les délais applicables (72 heures).

HONGRIE

En Hongrie, l'autorité chargée de veiller au respect du RGPD et du droit national est l'Autorité nationale hongroise pour la protection des données et la liberté d'information (*Nemzeti Adatvédelmi és Információszabadság Hatóság)*.

La Hongrie a révisé sa loi nationale sur la protection des données en deux temps. Deux lois ont été adoptées et sont entrées en vigueur en juin et juillet 2018.

Dans les pages suivantes, vous trouverez les résumés de trois décisions qui portent sur :

⇒ Une sanction pécuniaire de 35 000 euros à l'encontre d'un site internet géré par un parti politique pour manquement à son obligation de notification en cas de violation des données ;

⇒ Une sanction pécuniaire de 3 070 euros à l'encontre d'une société pour violation du droit à la limitation du traitement, du droit d'accès et de l'obligation d'informer la personne concernée de son droit d'introduire une réclamation auprès de l'autorité de contrôle ;

⇒ Un avertissement à l'encontre d'une société pour manquement à son obligation de disposer d'une base légale du traitement.

BUDAPEST

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire de 11 millions de HUF / environ 35 000 €	21 mars 2019	Manquement à l'obligation de notification d'une violation de données à l'autorité de contrôle (*article 33 du RGPD*) et aux personnes concernées (*article 34 du RGPD*)	L'autorité hongroise a reçu une plainte selon laquelle une base de données contenant les données à caractère personnel des adhérents d'un parti politique était librement accessible sur un forum pirate anonyme. Il s'agissait en particulier des adresses électroniques, des identifiants de connexion et des mots de passe. Par ailleurs, ces mots de passe n'étaient pas chiffrés de manière sécurisée. Le parti politique était au courant de la violation de données mais il n'en a pas informé l'autorité de contrôle hongroise ni les personnes concernées (environ 6000 personnes). Il faisait valoir qu'il n'était pas obligé de notifier la violation parce que les données en question n'étaient pas mises à jour. L'autorité estime que le fait que les données ne soient pas mises à jour est indifférent à l'égard de l'obligation de notification. Par ailleurs, elle considère que l'incident présentait un risque élevé car il a affecté les données de personnes qui sont ou pourraient être encore adhérents du parti politique. De plus, elle précise qu'il s'agit des catégories particulières de données (article 9 du RGPD) puisqu'elles révèlent les opinions politiques des personnes concernées et que cela constitue une circonstance aggravante. Par ailleurs, l'autorité considère que le parti politique utilisait une technologie de chiffrement obsolète pour sécuriser les mots de passe, ce qui entraine également un risque grave car la disponibilité publique de ces informations peuvent conduire à d'autres violations des services en ligne utilisés par les personnes concernées. Par conséquent, l'autorité a prononcé une sanction d'environ de 35 000 euros pour absence de notification d'une violation de données à risque élevé.

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire 1 000 000 de forins (FT) / environ 3070 €	21 décembre 2018	• Violation du droit à la limitation du traitement (*article 18, 1, c) du RGPD*) • Violation du droit d'accès, en particulier de fournir une copie des données à caractère personnel (*article 15, 3 du RGPD*) • Violation de l'obligation d'informer la personne concernée de son droit d'introduire une réclamation auprès de l'autorité de contrôle (*article 12,4 du RGPD*)	Une personne, qui s'était rendue dans les locaux d'une société, a souhaité ensuite exercer son droit d'accès aux données la concernant et son droit à la limitation du traitement, au regard d'un dispositif de vidéosurveillance. Plus précisément, la personne sollicitait du responsable de traitement qu'il lui fournisse une copie des enregistrements vidéos correspondant aux heures et lieux où elle s'était rendue dans les locaux de la société. Elle lui demandait également de ne pas supprimer ces enregistrements. Elle justifiait cette demande par son intention d'exercer une action en justice. La société a refusé, au motif que les conditions du RGPD permettant d'ouvrir droit à l'exercice du droit à la limitation du traitement (article 18, 1, c)) n'étaient pas remplies. Pour la société, la personne concernée ne fournissait pas de justification quant à la nécessité des enregistrements dans le cadre de son action. En effet, la société faisait valoir que les enregistrements ne comportaient que de l'image et non du son. Ainsi, cela permettait seulement de démontrer la présence de la personne dans les locaux et non la raison de sa venue ; ce qui était l'objet de son action en justice selon la société. Toutefois, l'autorité considère que l'article 18,1,c) n'exige pas de la part de la personne concernée d'apporter des preuves au responsable de traitement : il suffirait que la personne concernée soutienne que la limitation est nécessaire dans le cadre de sa démarche en justice. Il ne revient pas au responsable de traitement d'évaluer la pertinence de la démarche de la personne concernée. De plus, l'autorité rappelle que le droit de recevoir une copie des données, dans le cadre d'une demande de droit d'accès, peut être exercé sans condition. Par ailleurs, elle estime que le responsable de traitement a violé l'article 12,4 du RGPD puisque, dans sa réponse, il n'avait pas informé la personne concernée de son droit d'introduire une réclamation auprès de l'autorité de contrôle.

Décision	Date	Manquements relevés	Faits reprochés
Avertissement	21 mars 2019	Manquement à l'obligation de disposer d'une base légale (*article 5,1) a et article 6 du RGPD*)	En 2006, une personne a conclu un contrat de prêt avec une société. Ce contrat comportait une garantie au bénéfice de la société en cas de non-paiement, qui portait en l'espèce sur un bien immobilier. Toutefois, au moment de la rédaction du contrat, une adresse erronée avait été indiquée pour le bien en question. Cette erreur avait été rectifiée sur la version papier du contrat, mais pas dans sa version numérique. De ce fait, l'adresse contenue dans la base de données informatique de la société était inexacte. En 2018, la personne ne versait pas l'intégralité des montants dus. Un employé de la société a cherché donc alors à prendre contact avec le propriétaire du bien mentionné par erreur dans la base de données. L'employé de la société a téléphoné au tiers propriétaire de ce bien, à qui il a communiqué des informations relatives à la personne concernée, à ses dettes et au contrat. L'autorité de contrôle rappelle que la règlementation s'applique à tout type de traitements de données, qu'ils soient ou non automatisés. L'autorité indique que la communication de données par téléphone constitue bien un traitement, dépourvu en l'espèce d'une base légale. La société ayant immédiatement rectifié les données par la suite, l'autorité n'a pas infligé de sanction pécuniaire.

ITALIE

En Italie, l'autorité de protection des données est appelée *Garante per la protezione dei dati personali,* ou *Garante*.

Le cadre législatif italien relatif à la protection des données a été révisé par le décret n°101/2018, entré en vigueur le 19 septembre 2019. Il modifie certaines dispositions du décret n°196/2003 et en ajoute de nouvelles pour adapter le droit italien au RGPD.

A la page suivante, vous trouverez le résumé d'une décision prononçant une sanction pécuniaire de 50 000 euros à l'encontre d'un responsable du traitement en raison des mesures techniques et organisationnelles insuffisantes pour garantir la sécurité et la confidentialité des données.

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire de 50 000 euros	4 avril 2019	Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité et la confidentialité des données *(article 32, 1 du RGPD)*	Au cours de l'été 2017, une faille de sécurité avait été identifiée sur plusieurs sites reliés à un mouvement politique italien. A la suite d'une procédure de contrôle, l'autorité italienne avait identifié des défauts de sécurité et ordonné aux responsables des traitements concernés d'y mettre fin, notamment en prescrivant l'adoption d'une série de mesures correctrices sous trente jours, ainsi que le renforcement de la sécurité des systèmes d'information et la mise en conformité au RGPD (notamment au principe de minimisation) dans un délai plus long. Les responsables des traitements en cause avaient mis en place les mesures correctrices dans les délais. L'autorité a suivi la mise en conformité effective des responsables de traitements au RGPD, dans le cadre de contrôles ultérieurs. Par une décision du 4 avril 2019, l'autorité italienne constate que bien que des mesures de sécurité aient été mises en œuvre, il subsiste des manquements à l'obligation de sécurité, en particulier en raison de l'absence de traçabilité complète des accès à la base de données, du partage d'identifiants entre plusieurs personnes en charge de l'une des plateformes contrôlées, et de l'absence d'une politique de contrôle d'accès. Ces manquements ayant déjà été énoncés dans la procédure de contrôle initiale, l'autorité italienne prononce à l'encontre du responsable du traitement une sanction pécuniaire de 50 000 euros, en raison de la durée du manquement, du fait qu'il concerne des données relevant d'une catégorie particulière de données (opinion politique), qu'il touche un nombre significatif de personnes concernées et au regard du caractère obsolète et inadéquat des mesures de sécurité implémentées. Toutefois, l'autorité de contrôle note également les progrès en termes de sécurité depuis le contrôle initial, et le fait que le responsable de traitement soit une association et non une société.

LITUANIE

En Lituanie, le pouvoir de contrôle est partagé entre deux autorités. A côté d'une autorité de contrôle « classique » (similaire à la Cnil), il existe une autre autorité chargée de contrôler les traitements de données à caractère personnel à des fins journalistiques, académiques, artistiques ou littéraires. Dans l'exercice de ses pouvoirs, cette dernière doit coopérer avec la première.

La Lituanie a adopté le 30 juin 2018 une loi relative à la protection des données adaptant le droit national au RGPD. Cette loi remplace la loi antérieure au RGPD et elle est en vigueur depuis le 16 juillet 2018.

A la page suivante, vous trouverez la synthèse d'une décision prononçant une sanction pécuniaire de 61 000 euros à l'encontre d'une société de paiement électronique pour manquements aux principes de minimisation des données, de limitation de la durée de conservation, d'intégrité et de confidentialité des données. L'autorité reproche également à la société de ne pas avoir mis en œuvre des mesures techniques et organisationnelles suffisantes pour garantir la sécurité du traitement et de ne pas avoir notifié la violation des données.

VILNIUS

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire de 61 500 €	16 mai 2019	• Manquement aux principes de minimisation des données, de limitation de la durée de conservation et d'intégrité et de confidentialité des données (*article 5,1 du RGPD*) • Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement (*article 32,1 du RGPD*) • Manquement à l'obligation de notification de la violation de données (*article 33 du RGPD*)	Les données à caractère personnel des clients d'une société de paiement électronique ont été rendues publiques sur un site internet pendant au moins deux jours en juillet 2018. Le site contenait également plus de 9 000 captures d'écran présentant des informations sur les opérations de paiement des clients. L'origine de cette violation de données n'est pas connue de manière certaine. L'autorité de contrôle constate que la société n'a pas notifié la violation de données à l'autorité de contrôle et aux personnes concernées. Par ailleurs, elle précise que la société ne disposait pas des mesures techniques et organisationnelles suffisantes pour garantir la sécurité des données. En effet, un seul salarié s'occupait de la sécurité des systèmes d'information de la société. De plus, les données n'étaient pas chiffrées et il n'y avait pas de mesures de contrôle d'accès. Par ailleurs, la société collectait et traitait de manière régulière une quantité excessive de données. Outre les données aux opérations de paiement (nom, prénom, identifiant du client, numéro de compte etc.), la société collectait et traitait les factures électroniques (dates, données des expéditeurs, montants), les messages non lus (dates, sujets et une partie des textes) et d'autres informations sur les prêts, les pensions de retraite et les cartes de crédits de ses clients. En ce qui concerne la durée de conservation des données, fixée à dix minutes, la société avait conservé les données pendant 216 jours. En prenant en compte tous ces éléments, l'autorité de contrôle a prononcé une amende de 61 500 euros à l'encontre de la société. Cette sanction a fait l'objet d'une concertation avec l'autorité de protection de Lettonie.

MALTE

L'autorité de contrôle de la République de Malte est appelée *Information and Data Protection Commissioner*. Elle est chargée de s'assurer du respect du RGPD ainsi que de la loi maltaise relative à la protection des données, soit le *Data Protection Act 2018 (Chapter 586 of the Laws of Malta)*. Cette loi a remplacé l'ancien Data Protection Act *(Chapter 440 of the Laws of Malta).*

A la page suivante, vous trouverez le résumé d'une décision de cette autorité. Il s'agit d'une sanction pécuniaire de 5 000 euros prononcée à l'encontre de l'Autorité foncière maltaise en raison de mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement.

VALETTA

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire de 5 000 €	18 février 2019	Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement (*article 32 du RGPD*)	Le Commissaire à la protection des données maltais a ouvert une enquête sur l'Autorité foncière du pays, après les révélations du journal « The Times of Malta » le 23 novembre 2018 sur les manquements de l'Autorité à ses obligations concernant ses formulaires de demande en ligne. Le journal révélait que près de 10 gigaoctets de données à caractère personnel collectées par l'Autorité étaient librement accessibles sur internet. Cette fuite de données était due à un défaut de sécurisation du formulaire de collecte présent sur le site internet, par lequel des administrés pouvaient effectuer des demandes diverses. A l'issue d'un contrôle, le Commissaire a conclu que l'Autorité foncière ne disposait pas de mesures techniques et organisationnelles nécessaires pour garantir la sécurité du traitement de données à caractère personnel et n'avait donc pas respecté l'article 32 du RGPD. L'Autorité a été sanctionnée à hauteur de 5 000 euros.

POLOGNE

En Pologne, le Parlement a adopté le 12 septembre 2017 deux propositions de loi sur la protection des données à caractère personnel visant à adapter le droit polonais au RGPD. La première est entrée en vigueur le 25 mai 2018 tandis que la seconde n'a pas encore été adoptée définitivement.

Le première loi crée une nouvelle autorité de contrôle chargée de s'assurer du respect du RGPD et des lois nationales, appelée *Urzad Ochrony Danych Osobowych.* Cette autorité a plus de pouvoirs que l'ancienne. La deuxième loi, quant à elle, vise à mettre en place des dispositions spécifiques à chaque secteur d'activité (travail, banque, assurance, etc.).

A la page suivante, vous trouverez le résumé d'une décision prononçant une sanction pécuniaire de 220 000 euros à l'encontre d'une société pour manquement à son obligation d'information.

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire de 943 000 PLN / environ 220 000 €	Mars 2019	Manquement à l'obligation d'information (*article 14 du RGPD*)	Une société traitait des données collectées issues de sources publiques, à savoir le registre central électronique d'information sur les activités économiques (CEiDG, équivalent du Registre du commerce et des sociétés en Pologne). Toutefois, la société n'informait de ce traitement que les personnes concernées pour lesquelles elle disposait d'une adresse électronique. Pour les autres personnes concernées (adresses postales et numéro de téléphone), la société avait uniquement prévu une mention d'information sur son site internet. Pour justifier l'absence d'information directement délivrée à ces personnes, la société arguait du coût important qu'une telle information aurait générée (envoi de lettres recommandées à environ 6 millions de personnes). L'autorité polonaise estime que le RGPD n'imposait pas à la société d'informer les personnes par lettre recommandée et que les coûts n'étaient pas suffisamment élevés pour justifier l'absence d'information délivrée directement auprès des personnes concernées. Pour fixer l'amende, l'autorité polonaise souligne que la société avait conscience des obligations qui pesaient sur elle et que son manquement était intentionnel, qu'elle n'a pris aucune mesure pour mettre fin à la violation avant la sanction et qu'elle n'a pas indiqué vouloir le faire.

PORTUGAL

Au Portugal, l'autorité de contrôle chargée de s'assurer du respect du RGPD est appelée Comissão Nacional de Proteção de Dados ou CNPD.

Le Parlement portugais n'a pas encore adopté la loi destinée à adapter le droit portugais au RGPD. Il existe toutefois une loi relative à la protection des données, révisée notamment par une loi du 24 aout 2015. Elle ne reste en vigueur que pour les dispositions qui ne contredisent pas celles du RGPD.

Vous trouverez la synthèse d'une décision de la CNPD à la page suivante. Il s'agit de la première sanction prononcée en application du RGPD dans l'Union.

Une amende de 400 000 euros a été prononcée à l'encontre d'un hôpital en raison de manquements au principe d'intégrité et de confidentialité des données, au principe de minimisation des données et en raison de mesures techniques et organisationnelles insuffisantes pour garantir la sécurité de celles-ci.

Décision	Date	Manquements relevés	Faits reprochés
Sanction pécuniaire de 400 000 €	11 octobre 2018	• Violation du principe d'intégrité et de confidentialité des données (*article 5, 1 f du RGPD*) • Manquement au principe de minimisation des données (*article 5, 1 c du RGPD*) • Mesures techniques et organisationnelles insuffisantes pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement (*article 32, 1 b du RGPD*)	L'entité sanctionnée était un hôpital. La CNDP lui a reproché l'absence de mesures techniques et organisationnelles permettant de sécuriser les données des patients. Notamment : ◊ Des agents non habilités ont pu accéder à des données de patients, ce qui constitue une violation de données. ◊ Le personnel disposant d'un accès à la base de l'hôpital avait accès à l'intégralité des données de tous les patients (pas de différenciation des niveaux d'accès en fonction des besoins), et pouvait également accéder à des données de patients d'autres hôpitaux, sans que cela ne soit justifié. ◊ L'hôpital n'était pas en mesure d'assurer en continu la surveillance de son système d'information pour assurer l'intégrité et la confidentialité des données. L'hôpital s'est vu ainsi infligé une amende de 400 000 euros par la CNPD en raison de ces nombreux manquements.

REPUBLIQUE TCHEQUE

Le parlement tchèque a adopté en mars 2019 la loi destinée à adapter le droit national au RGPD. Selon cette loi, il n'est pas possible de prononcer des sanctions pécuniaires à l'encontre des autorités et organismes publics en cas de manquement au RGPD.

A la page suivante, vous trouverez deux décisions rendues par l'autorité de contrôle tchèque.

Dans la première, l'autorité a ordonné à un hébergeur de site internet (sous-traitant) situé aux Etats-Unis de cesser le traitement des données à caractère personnel, notamment pour manquement à l'obligation de disposer d'une base légale.

La seconde décision, quant à elle, porte sur un avertissement prononcé à l'encontre d'une société d'assurance pour violation du droit d'accès.

PRAGUE

Décision	Date	Manquements relevés	Faits reprochés
Cessation du traitement	14 janvier 2019	Manquement à l'obligation de disposer d'une base légale (*article 5,1) a et article 6 du RGPD*)	L'autorité de contrôle tchèque a annoncé le 14 janvier 2019 avoir fait fermer un site hébergé aux Etats-Unis, à destination d'un public tchèque, en raison des traitements illicites de données à caractère personnel mis en œuvre. Il s'agissait d'un site néo-nazi sur lequel des données à caractère personnel étaient régulièrement diffusées (noms, date de naissance, photo, adresse de personnes, copies de cartes d'identité, courriels piratés, etc.) En raison de l'anonymat des gérants du site, l'autorité de contrôle a pris contact avec l'hébergeur du site, soumis au RGPD en sa qualité de sous-traitant. Celui-ci a mis fin aux services d'hébergement lié au nom de domaine du site après que l'autorité l'ait averti que ce traitement constituait une violation du RGPD.
Avertissement	Inconnue	Non respect du droit d'accès (*article 15 du RGPD*)	Le client d'une société d'assurance a souhaité exercer son droit d'accès par courrier électronique. La société a refusé de traiter sa demande en estimant que ce moyen de communication ne permettait pas d'assurer de l'identité du client de manière certaine. Elle lui a ainsi demandé de fournir une pièce d'identité comportant sa signature certifiée avant de traiter sa demande. L'autorité de contrôle a considéré que la société avait violé l'article 15 du RGPD car l'exercice du droit d'accès par la personne concernée a été soumis à une condition injustifiée. L'autorité n'a pas prononcé de sanction pécuniaire au motif que la société a immédiatement remédié à son manquement en ouvrant droit à la demande

ROYAUME-UNI

Au Royaume-Uni, l'autorité de protection des données est appelée l'*Information Commissioner Office* ou l'*ICO*.

Pour adapter le droit national au RGPD, le Parlement britannique a adopté une loi relative à la protection des données (*Data Protection Act 2018*), entrée en vigueur le 25 mai 2018. La particularité de cette loi est qu'elle permet d'appliquer le RGPD au Royaume-Uni après sa sortie de l'Union européenne.

A la page suivante, vous trouverez le résumé de deux décisions rendues par l'*ICO* dans une même affaire. L'autorité a mis en demeure une entreprise canadienne d'arrêter le traitement et de supprimer les données à caractère personnel, pour manquements au respect des principes de licéité du traitement, de limitation des finalités, de minimisation des données et pour manquement à son obligation d'information.

Décision	Date	Manquements relevés	Faits reprochés
Mise en demeure	6 juillet et 24 octobre 2018	• Manquement à l'obligation de disposer d'une base légale (*article 5,1 a et article 6*) • Manquement au principe de limitation des finalités (*article 5, 1 b*) • Manquement au principe de minimisation des données (*article 5,1 c*) • Manquement à l'obligation d'information, dans le cadre d'une collecte indirecte (*article 14 et article 5,1, a*)	En mai 2017, l'*ICO* a lancé une procédure de contrôle relative à l'utilisation de données à caractère personnel dans le cadre des campagnes électorales. Selon l'autorité, une société canadienne était en relation contractuelle avec certaines organisations politiques britanniques. Ces dernières lui fournissaient des données à caractère personnel afin que la société canadienne cible les individus avec des publicités politiques via les réseaux sociaux. Pour l'autorité britannique, l'entreprise canadienne agit en tant que responsable de traitement. Si ces faits sont antérieurs à l'entrée en application du RGPD, le responsable du traitement a confirmé à l'autorité le 31 mai 2018 qu'il avait conservé ces données. Par une mise en demeure du 6 juillet 2018, l'autorité a notamment jugé que le responsable a violé les articles 5 (1)(a)-(c) et 6 du RGPD. Selon l'autorité, il a en effet traité des données à caractère personnel à l'insu des personnes concernées, pour des finalités auxquelles elles ne pouvaient s'attendre lors de la collecte initiale et sans base légale du traitement. Par ailleurs, le traitement était incompatible avec les finalités pour lesquelles les données ont été initialement collectées. Enfin, il n'avait pas fourni les informations prévues à l'article 14 (1) et (2) aux personnes concernées. L'autorité de contrôle a estimé qu'il était probable qu'un préjudice soit survenu pour les personnes concernées à la suite de ces manquements, en application de la section 150 (2) du Data Protection Act. Le 6 juillet 2018, l'autorité a mis en demeure le responsable du traitement de cesser tout traitement de données à caractère personnel des citoyens britanniques et européens sous 30 jours. Le 24 octobre 2018, l'autorité a publié une autre mise en demeure remplaçant la première. Elle a ainsi pris en compte l'enquête menée en parallèle par l'autorité régionale canadienne de protection des données sur cette même société, et a ordonné à celle-ci de supprimer les données à caractère personnel des citoyens britanniques qu'elle détenait.

Abonnez-vous à notre Newsletter :

www.avocats-mathias.com

Mathias Avocats

Nous sommes un cabinet spécialisé dans le droit du digital et accompagnons nos clients au gré des changements que le monde numérique implique.

Nos clients font partie de grands groupes ou sont des entreprises leaders dans l'innovation digitale. Nous représentons également des startups, au développement desquelles nous avons participé au fil des ans.

Les différentes décisions des autorités de contrôle européennes présentées dans ce Livre Blanc n'ont pas fait l'objet de traduction officielle.

Ce panorama présente nécessairement un caractère non-exhaustif. Les autorités de contrôle peuvent notamment rendre des décisions non publiques.

Mathias Avocats

Avez-vous une question ?

Une équipe dédiée pour vous accompagner dans la réalisation de vos ambitions.

01 43 80 02 01

contact@avocats-mathias.com

19, rue Vernier – 75017 Paris

Retrouvez les conseils pratiques de nos avocats sur Twitter :

@GaranceMathias