# NEWSLETTER RGPD

NUMÉRO 44 ● JUIN 2022


## ACTUALITES DU CABINET P. 15

**TABLE-RONDE SUR LE RAPPORT DE LA CNIL 2021**
**2 JUIN 2022**

**MATINALE - LA DATA : ENJEUX ET PERSPECTIVES**
**23 JUIN 2022**

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

## SOMMAIRE

## ACTUALITES

# GOOGLE ANALYTICS JUGÉ, UNE NOUVELLE FOIS, NON CONFORME AU RGPD PAR L'AUTORITÉ AUTRICHIENNE DE CONTRÔLE

*Par une décision du 22 avril 2022, l'autorité autrichienne de contrôle a de nouveau estimé que le transfert hors UE de données à caractère personnel opéré par la solution Google Analytics est contraire au RGPD.*

Après avoir conclu, dans une première décision du 22 décembre 2021, que l'utilisation de l'outil Google Analytics n'était pas conforme au RGPD (voir notre commentaire de la décision ici), l'autorité autrichienne de contrôle a reçu une plainte la conduisant à ouvrir une nouvelle enquête concernant l'outil Google Analytics.

Après avoir (i) rappelé que l'utilisation de Google Analytics engendre un traitement de données à caractère personnel, et (ii) qualifié l'éditeur du site de responsable du traitement et Google de sous-traitant, l'autorité de contrôle a accueilli favorablement la plainte en rappelant sa précédente décision dans laquelle elle concluait que *« l'obligation pour les responsables du traitement et les sous-traitants d'assurer un niveau de protection des personnes physiques [peut] être revendiqué comme un droit subjectif devant l'autorité de contrôle compétente ».*

Lors de l'enquête, Google s'est défendue en invoquant de nombreux arguments, dont certains sont inédits :

- Google a d'abord invoqué l'existence de mesures supplémentaires, et notamment (i) « *la publication d'un rapport de transparence »,* l'existence *« d'une politique de traitement des demandes gouvernementales* » ainsi que « *l'examen minutieux de toute demande d'accès aux données* », mais également (ii) la possibilité de crypter les données.

  L'autorité de contrôle a estimé ces mesures inutiles, car n'empêchant pas les autorités américaines d'accéder aux données personnelles. En ce qui concerne, plus précisément, le cryptage, ces mesures ont été considérées comme insuffisantes dès lors que Google « *a la possibilité d'accéder aux données en clair* ».

- Google a ensuite invoqué l'existence d'une « fonction d'anonymisation de l'adresse IP ».

  Cet argument n'a pas non plus convaincu l'autorité de contrôle qui a rappelé que *« l'adresse IP n'est masquée que dans un deuxième temps, après avoir été reçue par le réseau de collecte de données Analytics* », et qu'en tout état de cause, l'adresse IP n'est *« qu'une des nombreuses pièces du puzzle de l'empreinte numérique du plaignant ».*

- Enfin, Google a invoqué l'argument selon lequel une décision faisant droit à la plainte aurait de *« graves conséquences pour l'économie ».*

Face à cet argument, l'autorité de contrôle s'est contentée de rappeler qu'elle n'a pas *« à prendre en compte des considérations économiques ou politiques »* pour rendre ses décisions. L'autorité s'est uniquement basée sur l'aspect juridique, citant l'arrêt Schrems II de la CJUE, et rappelant que la situation juridique aux Etats-Unis n'est pas compatible avec le droit européen relatif à la protection des données.

Compte tenu de ce qui précède, et constatant que le transfert de données hors UE n'est encadré par aucune garantie appropriée, l'autorité de contrôle a estimé que l'outil Google Analytics n'est pas conforme au RGPD, et qu'il ne peut donc être utilisé en toute légalité.

L'autorité de contrôle n'a cependant prononcé aucune sanction, ni à l'encontre de l'éditeur du site, ni à l'encontre de Google :

- En ce qui concerne l'éditeur du site, l'autorité de contrôle a considéré que *« la violation de l'article 44 du RGPD [lui] est imputable* », mais n'a pas jugé nécessaire de le sanctionner dès lors que l'outil Google Analytics a été retiré avant que la décision n'intervienne.

- Google n'a pas non plus été condamnée dès lors que, comme l'a rappelé l'autorité de contrôle, « *les exigences du chapitre V du RGPD doivent être respectées par l'exportateur de données, mais pas par l'importateur de données* ».

**Source** : ici

# ASSOCIATIONS DE CONSOMMATEURS : LA CJUE OUVRE LA VOIE DES RECOURS POUR VIOLATION DU RGPD

*Par un arrêt du 28 avril dernier, la CJUE a jugé que les associations de consommateurs peuvent exercer des actions représentatives en violation du RGPD.*

Pour mémoire, conformément à l'article 80 paragraphe 1 du RGPD, la personne concernée peut mandater un organisme, une organisation ou une association pour qu'il/elle exerce une action en justice en son nom en cas d'atteinte à la protection de ses données à caractère personnel.

Aussi, selon l'article 80 paragraphe 2 du RGPD, les Etats membres peuvent prévoir que ce type d'entité, même indépendamment de tout mandat confié par une personne concernée, a le droit d'exercer une action en justice s'il considère que les droits d'une personne concernée prévus dans le RGPD ont été violés.

Dans cette affaire, les juges européens ont, plus précisément, été interrogés sur le point de savoir si une loi nationale peut autoriser une association de défense des intérêts des consommateurs à agir en justice contre l'auteur présumé d'une atteinte à la protection des données à caractère personnel :

- indépendamment d'une violation concrète du droit à la protection des données d'une personne concernée et, a fortiori, sans mandat de cette personne,
- en alléguant la violation d'autres règles juridiques visant à assurer la protection des consommateurs.

La CJUE répond par l'affirmative, considérant que le RGPD ne s'y oppose pas « *dès lors que le traitement de données concerné est susceptible d'affecter les droits que des personnes physiques identifiées ou identifiables tirent de ce règlement* ».

Sur le plan des principes, une association de consommateurs pourrait donc avoir un rôle majeur dans le contrôle du respect du RGPD.

En pratique, encore faut-il qu'une loi nationale, comme en Allemagne, prévoit effectivement l'exercice d'actions représentatives contre des violations des droits conférés par le RGPD par l'intermédiaire, le cas échéant, de règles ayant pour objet de protéger les consommateurs ou de lutter contre des pratiques commerciales déloyales.

Une voie ouverte aux réformes nationales ?

On sait déjà que les Etats membres doivent transposer avant la fin de l'année la Directive 020/1828 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs qui permettra aux associations de consommateurs, répondant à certains critères, d'engager des actions collectives contre l'auteur d'une atteinte à la protection des données personnelles.

Il serait donc possible d'aller plus loin avec une action complètement autonome des associations de consommateurs.

A suivre…

**Source** : ici

# LE CEPD PUBLIE SES LIGNES DIRECTRICES SUR L'UTILISATION DES TECHNOLOGIES DE RECONNAISSANCE FACIALE PAR LES AUTORITES REPRESSIVES ET JUDICIAIRES

*Constatant une utilisation de plus en plus intensive des technologies de reconnaissance faciale, le CEPD a publié des lignes directrices relatives à ces technologies qualifiées « d'outils sensibles susceptibles d'interférer avec les droits fondamentaux et d'affecter la stabilité politique, sociale et démocratique des pays ».*

Après avoir brièvement rappelé les différentes technologies de reconnaissance faciale, c'est-à-dire l'authentification (technique consistant à vérifier qu'une personne est bien celle qu'elle prétend être) et l'identification (technique consistant à retrouver une personne parmi un groupe d'individus), le CEPD est revenu sur l'implication et les dangers de ces technologies.

Le CEPD constate tout d'abord que l'utilisation des technologies de reconnaissance faciale engendre un traitement de quantités importantes de données à caractère personnel, y compris des données sensibles, le visage, et plus généralement les données biométriques, données intimement liées à l'identité d'une personne.

Par conséquent, l'utilisation de la reconnaissance faciale a un impact direct sur un certain nombre de droits et libertés fondamentaux consacrés par les textes, qui peuvent aller au-delà de la vie privée et de la protection des données.

Le CEPD est aussi conscient de la nécessité pour les autorités de bénéficier des meilleurs outils possibles pour identifier rapidement les auteurs de crimes.

Ainsi, compte tenu de ces observations, le CEPD rappelle que les outils de reconnaissance faciale doivent être utilisés dans le strict respect du cadre juridique applicable (notamment la directive « Police-Justice »[1]), et uniquement dans les cas où ils répondent aux exigences de nécessité et de proportionnalité. En d'autres termes, si ces solutions ont leur intérêt, elles ne doivent pas être considérées comme des « *solutions miracles* ».

C'est la raison pour laquelle le CEPD estime qu'il existe certains cas dans lesquels l'utilisation des technologies de reconnaissance faciale engendre des risques élevés inacceptables pour les individus et la société. Il s'agit de situations appelées « lignes rouges » que le CEPD appelle à interdire, comme par exemple :

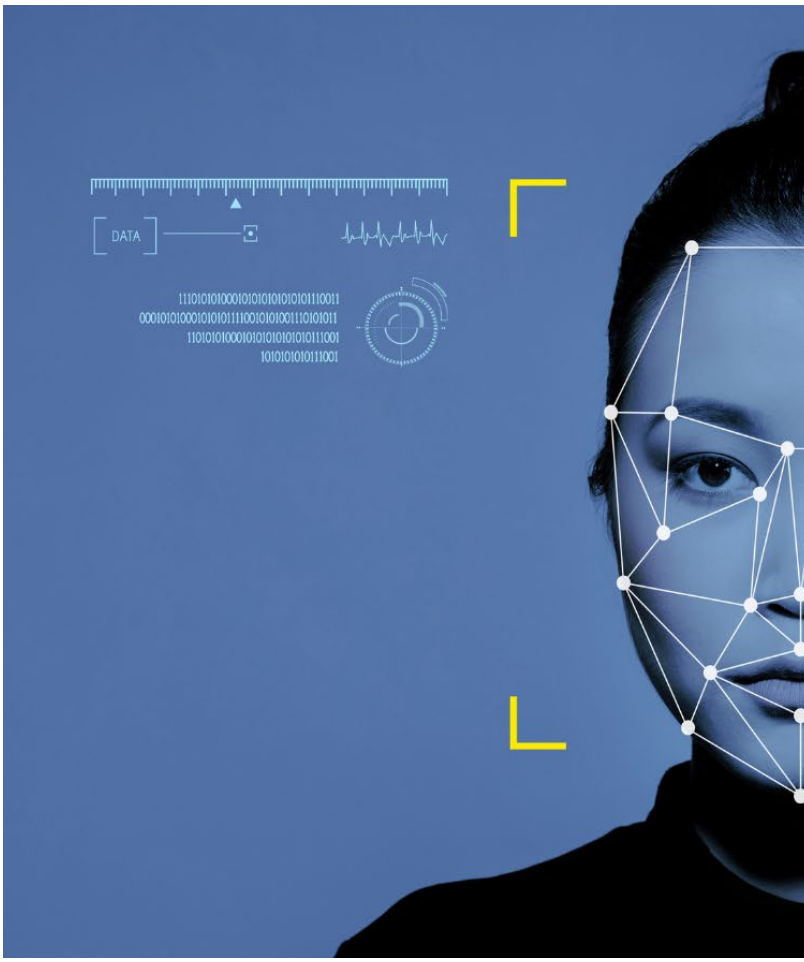
- l'identification à distance des personnes dans les espaces accessibles au public, impliquant une surveillance de masse ;

- les systèmes de reconnaissance faciale assistés par intelligence artificielle qui classent les individus sur la base de leurs données biométriques dans des groupes en fonction de leur origine ethnique, de leur sexe, de leur orientation politique ou sexuelle ;

- l'utilisation de la reconnaissance faciale pour déduire les émotions d'une personne (sauf exception dûment justifiée) ;

- le traitement de données à caractère personnel dans un contexte répressif qui s'appuierait sur une base de données alimentée par la collecte de données à grande échelle et de manière indiscriminée, par exemple en collectant des photographies et des images faciales accessibles en ligne, en particulier celles qui sont mises à disposition via les réseaux sociaux.

**Source** : ici




[1] DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

# LE CEPD PUBLIE SES LIGNES DIRECTRICES SUR LE CALCUL DES AMENDES ADMINISTRATIVES

*Le CEPD a élaboré des lignes directrices dans le but d'harmoniser les méthodes de calcul des amendes administratives au sein des différentes autorités de contrôle européennes.*

Soumises à consultation publique pendant 6 semaines avant adoption de leur version finale, l'objectif de ces lignes directrices est de créer des « points de départ harmonisés », à partir desquels le calcul des amendes administratives devra se fonder.

Ces lignes directrices sont complémentaires des « lignes directrices sur l'application et la fixation des amendes administratives »[1], préalablement publiées par le CEPD.

Rappelant (i) que le calcul du montant de l'amende est à la discrétion de l'autorité de contrôle et (ii) que le RGPD exige que le montant de l'amende soit efficace, proportionnel, dissuasif et individualisé, le CEPD a adopté une méthodologie en 5 étapes pour guider les autorités de contrôle dans la fixation du montant des amendes :

- La première étape consiste à identifier les opérations de traitement et évaluer s'il y a une ou plusieurs conduites sanctionnables, et si cette ou ces conduites donnent lieu à une ou plusieurs infractions.

- La deuxième étape consiste à trouver le point de départ pour le calcul de l'amende, c'est-à-dire la date à partir de laquelle toutes les circonstances de l'affaire doivent être prises en compte pour aboutir au montant final de l'amende.

- La troisième étape consiste à évaluer les circonstances aggravantes ou atténuantes. Il s'agit, notamment, selon le CEPD :

  - des mesures prises par le responsable du traitement ou le sous-traitant pour atténuer les dommages subis par les personnes concernées
  - du degré de responsabilité du responsable du traitement ou du sous-traitant
  - de l'existence d'infractions antérieures
  - du degré de coopération avec l'autorité de contrôle
  - de la manière dont l'infraction a été portée à la connaissance de l'autorité de contrôle
  - du respect des mesures ordonnées antérieurement concernant le même objet
  - de l'adhésion à des codes de conduite ou mécanismes de certification approuvés
  - de toute autre circonstance aggravante ou atténuante.

- La quatrième étape consiste à identifier les maximums légaux pertinents, notamment afin de vérifier que les amendes maximales ne sont pas dépassées.

- Enfin, la cinquième étape consiste à analyser si le montant final de l'amende répond aux exigences d'efficacité, de dissuasion et de proportionnalité exigé par le RGPD, quitte à augmenter ou diminuer l'amende en conséquence.

Comme le rappelle le CEPD, cette méthode « générale » poursuit des objectifs d'harmonisation et de transparence, mais ne doit pas être interprétée comme une formule mathématique et automatique, ces lignes directrices feront ainsi l'objet d'un examen régulier pour ajuster au mieux la méthode.

**Source** : ici

# DROIT D'ACCES: LA FIN DE L'ANONYMAT DU LANCEUR D'ALERTE ?


Le droit d'accès permet à toute personne, en application de l'article 15 du RGPD, de savoir si un organisme traite ses données et, dans l'affirmative, d'en obtenir la communication dans un format compréhensible. Il permet ainsi de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer.

En réponse à une demande de droit d'accès, l'organisme sollicité doit adresser à la personne concernée une copie des données qu'il détient et renseigner cette dernière sur notamment: les finalités d'utilisation de ses données, les catégories de données collectées, les destinataires qui ont pu accéder aux données, et la source des données si celles-ci n'ont pas directement été collectées par l'organisme.

Ce dernier, qui est tenu de répondre dans un délai de trente jours, ne peut s'opposer à une telle demande, sauf s'il considère, par exemple, que l'exercice du droit d'accès porte atteinte au droit des tiers[1].

L'organisme ne doit donc communiquer, pour préserver le droit des tiers, que les données qui concernent l'auteur de la demande de droit d'accès, à l'exclusion de toute autre donnée. A cet égard, la Cnil précise que « *l'exercice de ce droit ne peut pas se faire au détriment des autres personnes dont les données sont traitées.* »[2]

**L'affaire[3]**

A la suite de plusieurs plaintes concernant de fortes nuisances olfactives dans la cage d'escalier d'un immeuble d'habitation, un courrier fut adressé à un des locataires l'informant qu'une inspection serait réalisée.

Celle-ci ayant révélé un état négligé de l'appartement en cause, le locataire fut enjoint de le nettoyer et de le désencombrer. En réponse, et invoquant son droit d'accès, le locataire demanda notamment au syndic la communication de l'identité des personnes à l'origine des différentes plaintes le mettant en cause.

Le syndic ayant refusé de faire droit à cette demande, le locataire porta l'affaire devant la justice allemande. Débouté par les juridictions du premier et du second degré qui ont fait prévaloir les droits et libertés du lanceur d'alerte sur le droit d'accès du demandeur, ce dernier forma un pourvoi en cassation.

Selon la Cour fédérale, il s'agissait de savoir si l'intérêt du lanceur d'alerte au secret de son identité l'emporte sur l'obligation du responsable du traitement de fournir les informations requises au titre du droit d'accès :

« *L'obligation du responsable du traitement (...) de fournir à la personne concernée toutes les informations disponibles sur l'origine des données, vise à permettre à la personne concernée de faire valoir d'éventuels droits également à l'encontre de la personne ou de l'organisme d'où proviennent les données (éventuellement incorrectes ou divulguées à tort (...). En revanche, en faveur du lanceur d'alerte, il convient de rappeler que ses droits*

*au titre de l'article 7, paragraphe 1 (respect de la vie privée) et de l'article 8 (droit aux données à caractère personnel) de la Charte des droits fondamentaux (...) constituent une garantie uniforme de protection* ».

La haute juridiction précise à cet égard qu'*« il ne saurait être présumé que les informations demandées par le demandeur sur l'origine des données à caractère personnel traitées par le défendeur («fortes nuisances olfactives et vermine dans la cage d'escalier» relatives au domicile du demandeur) porteraient atteintes aux droits et libertés du lanceur d'alerte* ».

La Cour fédérale a ajouté que la charge de la preuve des circonstances pouvant justifier un refus de la demande de droit d'accès incombe au responsable du traitement.

Sur ces bases, et considérant que « *les intérêts ou les libertés et droits fondamentaux du lanceur d'alerte, qui exigent la protection ne prévalent pas »,* la Cour fédérale a annulé l'arrêt attaqué – faute de motivation suffisante - et renvoyé l'affaire devant la cour d'appel pour une nouvelle audience et une nouvelle décision.

**Quelles recommandations ?**

Il ne faut pas s'y méprendre. La Haute juridiction n'a pas, dans cette décision, fait prévaloir le droit à connaître la source des données (« droit d'accès ») sur le droit à l'anonymat du lanceur d'alerte (« droit des tiers »). Elle précise, en revanche, qu'il n'y a pas de hiérarchie établie entre les deux droits et que c'est au responsable du traitement, destinataire d'une demande de droit d'accès, de motiver sa décision lorsqu'il privilégie l'un à l'autre.

En somme, selon la haute juridiction allemande, il appartient à l'organisme sollicité de trouver un équilibre entre la satisfaction du droit d'accès du demandeur et le respect des droits et libertés des tiers.

Dans le cas d'espèce - le dépôt de plaintes par des habitants d'un immeuble visant un locataire - le syndic aurait probablement pu invoquer le « secret des correspondances » pour motiver son refus de divulguer l'identité des personnes à l'origine des plaintes.

Une telle motivation aurait probablement suffi pour justifier sa décision de ne pas faire droit totalement à la demande de droit d'accès du locataire.

Affaire à suivre …

**Alexandre FIEVEE**

[1] « Le droit d'obtenir une copie visé au para- graphe 3 ne porte pas atteinte aux droits et libertés d'autrui. » (RGPD, article 15)
[2] https://www.cnil.fr/fr/le-droit-dacces-des-sala- ries-leurs-donnees-et-aux-courriels-professionnels
[3] Cour fédérale, BGH, 22 février 2022, VI ZR 14/21, OLG Stuttgart.

# ACTUALITÉS EUROPÉENNES

## PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

### Une autorité de contrôle limite, dans l'urgence, un traitement de données pour garantir la vie privée et la dignité des personnes

*GPDP (Italie), 1er avril 2022*

*Dans une décision rendue le 1er avril 2022, l'autorité de contrôle italienne a limité, en urgence, un traitement de données personnelles portant atteinte à la vie privée et la dignité de personnes concernées.*

A la suite de la révélation d'une relation amoureuse entre un directeur de lycée et un élève de 18 ans, un média dévoilait, dans un article publié en ligne le 31 mars 2022, les messages personnels échangés entre les deux individus.

L'article, identifiant le directeur par son nom et une photo, et l'élève par ses initiales, s'attardait notamment sur le contenu de ces messages.

Saisie en urgence de cette affaire, l'autorité de contrôle s'est prononcée dès le lendemain.

Après avoir rappelé que la diffusion de données à caractère personnel à des fins journalistiques se heurte à d'autres droits et qu'ainsi l'information divulguée doit concerner des faits « *d'intérêt public* » revêtant un « *caractère essentiel* », l'autorité de contrôle a mentionné la nécessité, en l'espèce, de « *garantir la vie privée et la dignité des personnes concernées en prenant des mesures urgentes pour limiter la diffusion ultérieure de données à caractère personnel* ».


En conséquence, l'autorité de contrôle a fait usage de l'article 58 du RGPD qui lui permet notamment d'adopter des mesures correctrices en imposant une « *limitation temporaire du traitement* » à effet immédiat. Dans les faits, cette limitation a eu pour conséquence le retrait de l'article et l'interdiction de toute diffusion ultérieure du contenu des messages et des autres données personnelles des deux individus.

**Source** : ici

# Sanction d'un employeur divulguant les données personnelles de son ancienne salariée

*AEPD (Espagne), 28 avril 2022*

*Dans une décision rendue le 28 avril 2022, l'autorité de contrôle espagnole a considéré qu'un employeur ne peut pas relater sur internet les conditions de départ de l'entreprise d'une ancienne salariée en l'identifiant nommément.*

En réponse aux avis publiés sur Google critiquant son établissement, le propriétaire d'un café, ayant récemment licencié une de ses salariés, laissait notamment le commentaire suivant :

« *Le fait que vous soyez un ami de Mme X, qui en plus d'être licenciée (…) a été sanctionnée pour avoir commis des fautes graves pour des motifs déshonorants (…) ne vous donne pas le droit de porter atteinte à la réputation de l'établissement (…)* ».

Reprochant à son ancien employeur la divulgation de son nom, son prénom, les raisons de son départ (le licenciement) et l'existence d'une sanction professionnelle, la personne visée par ce commentaire a déposé une plainte auprès de l'autorité de contrôle espagnole.

Au cours de son enquête, cette dernière a considéré (i) que la divulgation de telles données constitue un traitement non autorisé, et porte ainsi atteinte au principe de confidentialité posé à l'article 5 du RGPD, et (ii) que le traitement effectué par l'employeur ne reposait sur aucune base légale (notamment ni le consentement et ni l'intérêt légitime), en contradiction avec l'exigence de base légale posée à l'article 6 du RGPD.


Compte tenu de ce qui précède, l'autorité de contrôle a infligé à l'ancien employeur une amende de 1.500 € et l'a enjoint à mettre en œuvre les mesures correctives nécessaires, notamment en supprimant les données personnelles publiées dans les commentaires.

**Source** : ici

# Attention à ne pas supprimer les données personnelles en cas de litige

*AZOP (Croatie), 8 mars 2022*

*Dans une décision rendue le 8 mars 2022, l'autorité de contrôle croate a considéré qu'un responsable du traitement ne peut pas refuser (i) l'accès aux images de vidéosurveillance puis (ii) les supprimer, lorsqu'un litige avec un consommateur est déclaré.*

Un usager mécontent des services d'une station essence a effectué une réclamation auprès du service client de cette dernière. Afin de « mieux protéger ses droits de consommateur », l'usager a également exercé son droit d'accès pour obtenir la copie des images de vidéosurveillance de la station essence.

Dans un premier temps, le responsable de la station essence a rejeté la demande au motif que cette dernière, effectuée sans demande écrite des autorités compétentes et sans justification, était susceptible de porter atteinte aux droits et libertés des clients et employés de la station essence.

Dans un second temps, enjoint par l'autorité de contrôle croate de fournir les enregistrements sollicités, la station essence a répondu que lesdits enregistrements avaient été effacés automatiquement au bout de 7 jours et qu'ainsi il était impossible de répondre favorablement à la demande d'accès de l'usager.

Entrant en voie de condamnation, l'autorité de contrôle a considéré qu'en ne fournissant pas l'enregistrement puis en le supprimant ultérieurement, le responsable du traitement avait :

- supprimé des éléments de preuve potentiellement importants dans le cadre de la procédure, et ;
- indirectement évité un préjudice financier qu'il pouvait subir à l'occasion de la réclamation.

Compte tenu de ce qui précède, et souhaitant dissuader d'autres responsables du traitement de supprimer des données en violation du RGPD, l'autorité de contrôle a infligé au responsable de la station essence une amende de près de 125 000 €.

**Source** : ici

# Pas de droit d'accès si la demande est disproportionnée

*AG Pankow (Allemagne), 28 mars 2022*

*Dans une décision rendue le 28 mars 2022, une autorité de contrôle allemande a considéré qu'il est possible, dans certaines situations, de refuser de répondre favorablement à une demande de droit d'accès, notamment lorsque la demande est disproportionnée*.

Un individu avait demandé à l'exploitant d'un réseau de transport de lui fournir la vidéo de la caméra de surveillance concernant l'un de ses trajets.

L'exploitant, considérant que la réponse à une telle demande allait engendrer une « dépense considérable de temps, d'argent et de main d'œuvre » avait refusé d'y faire droit.

L'individu a déposé une plainte auprès de l'autorité compétente qui, au terme de son analyse, a estimé qu'un responsable du traitement ne peut refuser de répondre à une demande de droit d'accès (en vertu de l'article 15 du RGPD) que s'il existe une « disproportion manifeste » entre, d'une part, l'effort requis et, d'autre part, l'intérêt pour la personne d'accéder aux données.

Cette solution est conforme au considérant 62 du RGPD, selon lequel :

*« Il n'est pas nécessaire d'imposer l'obligation de fournir des informations lorsque la personne concernée dispose déjà de ces informations, lorsque l'enregistrement ou la communication des données à caractère personnel est expressément prévu par la loi ou lorsque la communication d'informations à la personne concernée se révèle impossible ou exigerait des efforts disproportionnés ».*


Selon l'autorité de contrôle, dans la mesure où l'individu savait qu'il était filmé lors de son trajet, il avait donc connaissance tant de l'existence du traitement que de son contenu. Aussi, puisque le droit d'accès a pour objectif permettre aux personnes concernées de savoir si leurs données personnelles font l'objet d'un traitement, l'individu avait un intérêt *« extrêmement faible »* à accéder aux images.

En conséquence, la plainte de l'individu a été rejetée.

**Source** : ici

# ACTUALITÉS DU CABINET



Sur inscription préalable par email dpj@derriennic.com

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

## OBJECTIFS

1/ Acquérir les compétences, les connaissances et le savoir-faire attendus par la CNIL et permettre au collaborateur de se présenter à l'examen de certification en maximisant ses chances de succès.

2/ Indépendamment de la certification, la formation permet à l'apprenant de se familiariser avec la matière et d'acquérir les compétences, les connaissances et le savoir-faire pour :

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

## CONTENU DE LA FORMATION

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

## COÛT

**3000€ HT/personne**

## INTERVENANT

**Alexandre FIEVEE**
Avocat Associé
01.47.03.14.94
afievee@derriennic.com

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

RENSEIGNEMENTS PRATIQUES
**Prochaine session en 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 :**