Chambre Contentieuse

Décision quant au fond 18/2020 du 28 avril 2020

Numéro de dossier : AH-2019-0013

Objet : Rapport d'inspection relatif à la responsabilité des fuites de données et la position du délégué à la protection des données

La Chambre Contentieuse de l'Autorité de protection des données, constituée de Monsieur Hielke Hijmans, président, et de Messieurs Dirk Van Der Kelen et Jelle Stassijns, membres ;

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données)* (ci-après le "RGPD") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, ci-après la "LCA" ;

Vu le règlement d'ordre intérieur tel qu'approuvé par la Chambre des représentants le 20 décembre 2018 et publié au *Moniteur belge* le 15 janvier 2019 ;

Vu les pièces du dossier ;

a pris la décision suivante concernant :

Y, ci-après "le défendeur"

1. Faits et procédure

A. Enquête du Service d'Inspection

Le 11 juillet 2019, le Comité de direction de l'Autorité de protection des données (ci-après l'APD) a décidé de saisir le Service d'Inspection de l'APD de l'affaire sur la base de l'article 63, 1° de la LCA.

Après examen du dossier par le Service de Première Ligne, il s'avère en effet que trois points sérieux compromettent un respect correct du RGPD :

1. le non-respect de l'obligation de coopération (article 31 du RGPD) ;
2. le non-respect de la responsabilité (article 5.2 du RGPD) et de l'obligation de coopération (article 31 du RGPD) en ce qui concerne l'application de l'approche basée sur les risques ("risk based approach") dans le cadre de la sécurité des données à caractère personnel (article 36 du RGPD) ;
3. le non-respect de l'obligation du défendeur d'éviter un conflit d'intérêts dans le chef du délégué à la protection des données (article 38.6 du RGPD) et le fait que le délégué à la protection des données ne soit pas suffisamment impliqué (article 38.1 du RGPD).

Le motif de la saisine susmentionnée était une fuite concrète de données au niveau du défendeur. Cette fuite a également été appelée l'incident W. Cette fuite de données a eu lieu dans le cadre de plusieurs invitations qui ont été envoyées par le défendeur notamment à des indépendants et à des personnes exerçant une profession libérale afin de passer d'une facturation papier à une facturation électronique. Suite à une erreur dans la sélection des adresses e-mail, plusieurs invitations liées à des personnes exerçant une profession libérale et à des indépendants (et ensuite également la facture électronique) ont été envoyées à des adresses e-mail secondaires liées, dans les bases de données du défendeur, à un client mais n'ayant potentiellement aucun lien direct avec le client concerné. Ces personnes de contact secondaires sont des personnes de contact administratives ou techniques pour le client.

Les communications menées autour de cette fuite de données entre le Service de Première Ligne de l'APD et le défendeur ont donné lieu à une note soumise par le Service de Première Ligne au Comité de direction, contenant une proposition d'évaluer l'existence d'indices sérieux et de soumettre ensuite le dossier au Service d'Inspection afin de faire examiner la manière dont le défendeur traite les fuites de données (article 63, 1° de la LCA).

Le Service d'Inspection a transmis son rapport du 6 septembre 2019 à la Chambre Contentieuse sur la base de l'article 91, § 2 de la LCA, impliquant la saisine de la Chambre Contentieuse en vertu de l'article 92, 3° de la LCA.

B. Procédure devant la Chambre Contentieuse

En séance du 24 septembre 2019, la Chambre Contentieuse a décidé, en vertu de l'article 95, § 1er, 1° de la LCA, que le dossier pouvait être traité sur le fond.

Le même jour, le défendeur a été informé par courrier recommandé de cette décision ainsi que du rapport d'inspection et de l'inventaire des pièces du dossier qui a été transmis à la Chambre Contentieuse par le Service d'Inspection. De même, le défendeur a été informé des dispositions de l'article 98 de la LCA et, en vertu de l'article 99 de la LCA, il a été informé des délais pour introduire ses conclusions. La date limite pour la réception des conclusions en réponse du défendeur a été fixée au 28 octobre 2019.

Le 29 octobre 2019, la Chambre Contentieuse a reçu les conclusions en réponse de la part du défendeur. Outre la défense substantielle concernant les trois constatations du Service d'Inspection relatives à l'obligation de coopération (1), à la responsabilité du responsable du traitement (2) et à la position du délégué à la protection des données (3), ces conclusions contiennent aussi un moyen de défense procédural dans lequel le défendeur objecte que dans ce dossier, la répartition de compétences délimitée par le législateur entre le Service de Première Ligne et le Service d'Inspection n'a pas été respectée, ce qui conduirait à l'incompétence de la Chambre Contentieuse et à l'irrecevabilité du rapport du Service d'Inspection et de la note interne du Service de Première Ligne.

Le 14 février 2020, le traitement du dossier est repris et l'audition a lieu. Le défendeur est donc entendu et a la possibilité d'exposer ses arguments.

Ensuite, l'affaire est délibérée par la Chambre Contentieuse.

En vertu de l'article 54 du règlement d'ordre intérieur de l'Autorité de protection des données, une copie du procès-verbal de l'audition est transmise au défendeur le 18 février 2020.
Le défendeur se voit ainsi offrir l'opportunité de faire ajouter ses éventuelles remarques à cet égard en annexe du procès-verbal, sans que cela implique une réouverture des débats.

Le 21 février 2020, la Chambre Contentieuse reçoit du défendeur quelques remarques relatives au procès-verbal, remarques qu'elle décide de reprendre dans sa délibération et dans sa décision.

Le 26 février 2020, comme cela lui avait été demandé lors de l'audition, le défendeur transmet le numéro d'entreprise correct et le chiffre d'affaires annuel des trois derniers exercices Ce chiffre d'affaires est de :

pour 2017 : 4.058.643.958 €
pour 2018 : 4.009.935.363 €
pour 2019 : 3.886.699.793 €.

Le 3 avril 2020, la Chambre Contentieuse fait connaître au défendeur son intention de procéder à l'imposition d'une amende administrative, ainsi que le montant de celle-ci afin de donner au défendeur l'occasion de se défendre avant que la sanction soit effectivement infligée et exécutée.

Le 24 avril 2020, la Chambre Contentieuse reçoit la réaction du défendeur concernant l'intention d'infliger une amende administrative, ainsi que le montant de celle-ci. Le défendeur dit ne pas être d'accord avec l'imposition d'une amende ou avec le montant envisagé de l'amende et il renvoie à cet effet à ses conclusions. Toutefois, il n'avance aucun (nouvel) argument pour étayer cette position. Dès lors, aux yeux de la Chambre Contentieuse, la réaction du défendeur ne donne pas lieu à une adaptation de l'intention d'infliger une amende administrative, ni à une modification du montant de l'amende tel qu'envisagé.

2. Base juridique

Article 38.6 du RGPD

"6. Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts."

3. Motivation

a) Procédure

Comme premier moyen de défense, le défendeur avance que la procédure présenterait plusieurs manquements. Le défendeur objecte que le Service de Première Ligne est allé plus loin que le simple traitement du dossier de notification, si bien que l'on ne retrouve plus aucune trace de l'incident W dans les objections à l'origine de la procédure devant la Chambre Contentieuse. Selon le défendeur, il ressort de la demande de renseignements par écrit, plus précisément de l'ampleur des questions et

du nombre de questions complémentaires, que le Service de Première Ligne a mené une enquête, ce qui, conformément à l'article 66, § 1er, 3° de la LCA, relève de la compétence d'enquête du Service d'Inspection.

Le Service de Première Ligne aurait également fait usage de la modalité d'enquête pour identifier des personnes, ce qui relève de la compétence du Service d'Inspection (article 66, § 1er, 1° de la LCA). Le défendeur affirme que son argumentation – à savoir que l'enquête a déjà été menée au niveau du Service de Première Ligne et donc avant que le dossier ne parvienne au Service d'Inspection – est confirmée par le fait que pour les "*mesures d'enquête liées à l'enquête*", le rapport du Service d'Inspection renvoie exclusivement à l' "*analyse du dossier reçu via le Comité de direction*" [NdT : tous les passages issus du rapport d'inspection sont des traductions libres réalisées par le Secrétariat de l'Autorité de protection des données, en l'absence de traduction officielle]. Selon le défendeur, le Service d'Inspection base donc son rapport simplement et uniquement sur une enquête qui a été menée par le Service de Première Ligne.

Lors de l'audition, le défendeur ajoute à cela que la note interne émanant du Service de Première Ligne, qui a été adressée au Comité de direction et donc au moment où le Service d'Inspection n'avait pas encore été saisi du dossier, avait déjà été envoyée avec la mention des coordonnées du Service d'Inspection (inspection@apd-gba.be). La réalisation d'actes d'enquête par un service qui ne peut légalement pas les effectuer est qualifiée de fishing expedition par le défendeur.

Selon le défendeur, le Service de Première Ligne a dès lors outrepassé sa compétence et ne s'en est pas tenu à ses compétences légales, plus précisément sa compétence de lancer une procédure de médiation (article 22, 2° de la LCA). Le défendeur affirme que le Service de Première Ligne n'a pas accédé à ses multiples demandes de concertation.

En outre, selon le défendeur, le Service d'Inspection n'a pas non plus respecté ses compétences étant donné qu'il s'est exclusivement basé sur le dossier du Service de Première Ligne pour rédiger le rapport. Cela amène le défendeur à affirmer que le Service d'Inspection n'a mené aucune enquête car aucune des mesures d'enquête reprises à l'article 66, § 1er de la LCA n'a été prise. Le défendeur argumente que le Service d'Inspection n'était donc pas compétent pour rédiger son rapport, vu qu'il n'a pas pu clôturer son enquête de manière licite, en raison de l'absence de la moindre mesure d'enquête.

Le défendeur affirme que la Chambre Contentieuse n'a pas été saisie de manière valable en droit et doit se déclarer incompétente car :

- le Service d'Inspection n'a mené aucune enquête ;
- le Service d'Inspection n'était pas compétent pour clôturer son enquête ;

- la Chambre Contentieuse ne pouvait être saisie qu'après une clôture licite de l'enquête.

À titre subsidiaire, le défendeur objecte que le rapport du Service d'Inspection et la note interne du Service de Première Ligne ne peuvent être admis en raison d'une violation des principes de droit fondamentaux, en particulier du principe d'une procédure régulière et du droit de la défense, ainsi que des principes généraux de bonne gouvernance, dans le cadre desquels la Chambre Contentieuse, en tant qu'autorité administrative, doit en particulier respecter les principes de précaution et d'impartialité.

Au cours de l'audition, le défendeur ne nie pas qu'une enquête a été menée mais il prétend que cela s'est fait de la mauvaise façon. Le défendeur avance que la Chambre Contentieuse n'est pas compétente lorsque les éléments collectés ont été obtenus d'une manière légalement incorrecte. Selon le défendeur, les documents du Service de Première Ligne doivent dès lors être exclus de l'enquête et il souligne que le Service de Première Ligne doit intervenir dans le cadre de ses compétences comme cela est défini à l'article 22 de la LCA. Selon le défendeur, le respect de ce principe est essentiel en vue d'une sécurité juridique. Le défendeur affirme explicitement qu'il est important pour une entreprise de pouvoir dialoguer avec un département au sein de l'APD sans qu'une enquête soit d'emblée menée, de manière à permettre la collaboration, la concertation et la médiation.

La Chambre Contentieuse souligne qu'un traitement impartial et loyal doit être assuré tout au long du parcours. Le problème soulevé par le défendeur concerne la phase préalable, mais les droits de la défense n'ont pas été violés, car le défendeur a eu l'opportunité d'avancer son argumentation dans son intégralité au moyen de ses conclusions en réponse et il a en outre pu exercer pleinement son droit à la contradiction lors de l'audition de la Chambre Contentieuse.

La Chambre Contentieuse ne peut que constater que dans le cas où l'APD peut intervenir d'office, la procédure légalement prévue a été respectée, à savoir que lorsque le Comité de direction constate des indices sérieux de l'existence d'une pratique susceptible de donner lieu à une infraction aux principes fondamentaux de la protection des données à caractère personnel, dans le cadre de la LCA et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel, la saisine du Service d'Inspection peut avoir lieu (article 63, 1° de la LCA). En application de ce qui précède, en vertu de la décision du Comité de direction prise le 11 juillet 2019, le Service d'Inspection a été saisi du dossier le 12 août 2019, sans qu'une règle de procédure qui serait de nature à nuire aux intérêts du défendeur ou à violer ses droits ne soit violée. La garantie procédurale fondamentale consistant à assurer le droit à la contradiction a été respectée étant donné que le rapport d'inspection a été transmis par la Chambre Contentieuse au défendeur et qu'il a eu l'occasion de réagir à chacune des constatations formulées par le Service d'Inspection dans ce rapport.

La Chambre Contentieuses estime dès lors que la présente notification d'une éventuelle violation de données à caractère personnel a été traitée dans le respect de tous les principes de droit fondamentaux et des principes généraux de bonne gouvernance.

b) Coopération avec l'autorité de contrôle (article 31 du RGPD)

Concernant l'obligation de coopération, le Service d'Inspection établit la constatation suivante dans son rapport :

"Le défendeur a utilisé différents moyens pour compliquer la coopération obligatoire avec l'APD. Ces moyens sont décrits sur les pages Internet http://www.aalep.eu/recognizing-your-opposition-tactics-and-responding-them et https://ctb.ku.edu/en/table-of-contents/advocacy/ respond-to-counterattacks/ overview-of-opposition-tactics/main comme étant les "Ten D's".

Dans le cadre d'une évaluation des contacts avec le défendeur, on peut constater que le défendeur appliquait 5 des 10 techniques.

Selon le Service d'Inspection, il appartient à la Chambre Contentieuse d'établir si l'application des techniques susmentionnées constitue une violation de l'obligation de coopération ou peut être considérée comme un exercice normal du droit de la défense du défendeur sur la base des principes de droit généraux applicables."

Concernant ces constatations du Service d'Inspection en matière de coopération, le défendeur avance tout d'abord que vu que le Service de Première Ligne a outrepassé sa compétence et n'a donc pas rempli les missions qui lui étaient attribuées, il ne devait pas coopérer et ne devait pas accéder aux demandes du Service de Première Ligne. Deuxièmement, le défendeur conteste la valeur juridique des pages Internet sur lesquelles l'APD se base et il argumente qu'il a bel et bien apporté sa coopération et n'a appliqué aucune des cinq techniques "Ten D's". Le défendeur affirme que l'exigence de coopération est quoi qu'il en soit limitée par le droit de la défense et le droit à ne pas s'incriminer soi-même, qui s'applique dans les procédures administratives pouvant donner lieu à l'imposition d'amendes administratives. Les interrogations poussées violeraient le droit de la défense et l'interdiction d'auto-incrimination.

La Chambre Contentieuse a évalué les constatations du Service d'Inspection à la lumière de l'obligation de coopération du défendeur et constate que le Service d'Inspection n'a pas démontré suffisamment que le défendeur n'avait pas tenté par le biais de lettres de réponse de répondre de manière détaillée et circonstanciée aux questions posées. En outre, le défendeur s'est déclaré à plusieurs reprises disposé à engager une concertation, en complément de cette approche. On ne peut donc pas établir

qu'il n'a pas tenu compte de l'obligation de coopération avec l'autorité de contrôle.

La Chambre Contentieuse estime donc qu'**aucune violation de l'article 31 du RGPD** ne peut être constatée. Ce jugement se base sur des constatations de faits, rendant inutile un jugement de principe dans cette affaire concernant la portée de l'obligation de coopération.

c) Responsabilité (article 5.2 du RGPD et article 24, paragraphe 1 du RGPD) en ce qui concerne l'application de l'évaluation des risques lors de la notification d'une violation de données à caractère personnel (article 33 du RGPD)

Concernant ces indices sérieux du Comité de direction, le rapport d'inspection mentionne la constatation suivante :

"L'évaluation des risques par le défendeur lors de la notification de violations de données à caractère personnel était systématiquement "faible" ou "négligeablement faible" au cours de l'année passée. La manière dont l'équipe du défendeur (composée de représentants du business) est arrivée à ce résultat, malgré les questions posées à cet égard par l'APD, n'est pas claire concrètement. Comme cela ressort du courrier du défendeur du 12/06/2019, il n'est pas disposé à expliquer davantage cet aspect car il n'y serait pas obligé en vertu du RGPD. Il ressort en outre de la "matrice RACI" évoquée dans le courrier susmentionné que le délégué à la protection des données du défendeur ne participe pas aux discussions relatives à l'évaluation des risques en la matière étant donné qu'il est uniquement "informed" plutôt que "consulted". Qui décide quoi au sein du défendeur dans un dossier concret n'est pas communiqué à l'APD et il n'y a aucune indication selon laquelle le défendeur souhaite modifier cette pratique.
En raison de l'utilisation de descriptions vagues du processus d'évaluation et de négations, il est impossible à l'APD de vérifier de quelle manière le défendeur arrive à une certaine conclusion en matière de risques dans un dossier concret.
La méthode susmentionnée est contraire à la responsabilité (article 5, paragraphe 2 du RGPD) et à la responsabilité (article 24, paragraphe 1 du RGPD) du défendeur en ce qui concerne l'application de l'approche basée sur les risques dans le cadre de la sécurité des données à caractère personnel (article 32 du RGPD)."

Le défendeur fait remarquer que le rapport d'inspection renvoie uniquement explicitement à l'approche basée sur les risques dans le cadre de la *sécurité* des données à caractère personnel (article 32 du RGPD) alors qu'il ressort du contenu du rapport qu'il s'agit de l'évaluation des risques lors de la *notification de violations* de données à caractère personnel, ce qui concerne les articles 33 et 34 du RGPD, mettant ainsi le défendeur dans l'impossibilité de bien se défendre, ce qui implique des

conséquences pour la décision de la Chambre Contentieuse du point de vue des principes de droit fondamentaux et des principes généraux de bonne gouvernance.

Sur ce point, la Chambre Contentieuse estime qu'abstraction faite de cette constatation du défendeur concernant les articles de loi applicables, les conclusions du défendeur ne contiennent pas le moindre élément révélant qu'il se défend aussi concernant l'approche basée sur les risques dans le cadre de la *sécurité* des données à caractère personnel (article 32 du RGPD). La défense intégrale concerne l'évaluation des risques lors de la *notification de violations* de données à caractère personnel (articles 33 et 34 du RGPD). Aucun élément ne révèle que dans le chef du défendeur, il existait le moindre doute quant aux articles à l'origine de la constatation du Service d'Inspection, de sorte que sur cette base, on doive conclure que les principes de droit fondamentaux et les principes généraux de bonne gouvernance ont été respectés. Ceci s'explique par le fait que toutes les pièces du dossier concernent l'évaluation des risques lors de la notification de violations de données à caractère personnel. Le rapport d'inspection aussi mentionne au début de la constatation que cela concerne l'évaluation des risques lors de la notification de violations de données à caractère personnel et il ressort clairement du contexte du rapport qu'il ne s'agit que de cela.

Sur le plan du contenu, le défendeur affirme qu'il n'y a pas d'obligation légale de soumettre une possibilité de vérification détaillée à l'APD. Des informations relatives à la méthodologie pour l'analyse des risques et à la procédure relative à cette analyse et au processus décisionnel ont bel et bien été fournies à l'APD. En dépit de la contestation de la compétence de l'APD, le défendeur souligne que des informations ont quand même été fournies, dans le cadre desquelles il indiquait vouloir engager le dialogue concernant l'évaluation des risques. Le défendeur réagit aussi à la position du Service d'Inspection selon laquelle en utilisant des descriptions vagues du processus d'évaluation et des négations, le défendeur empêche l'APD de vérifier de quelle manière le défendeur en est arrivé à une certaine conclusion dans un dossier concret.

Le défendeur fait référence dans ses conclusions aux pièces pertinentes qui infirmeraient cette position du Service d'Inspection et qui permettraient ainsi à l'APD de quand même vérifier de quelle manière le défendeur en est arrivé à une certaine conclusion en matière de risques dans un dossier concret. Le défendeur conclut qu'il n'y a pas violation de la responsabilité, étant donné que l'article 5.2 du RGPD ne concernerait que les principes mentionnés à l'article 5.1 du RGPD et pas les règles relatives aux conséquences d'une violation de données à caractère personnel.

La Chambre Contentieuse souligne que contrairement à ce que le défendeur affirme, il y a bel et bien dans le chef du responsable du traitement une obligation de documenter chaque fuite de données, qu'elle comporte des risques ou non, afin de pouvoir fournir des informations à l'APD. En outre, contrairement aussi à ce que le défendeur affirme, l'article 5.2 du RGPD ne se limite pas aux principes

énumérés à l'article 5.1 du RGPD mais concerne bel et bien aussi les autres dispositions du RGPD, dont l'article 33 du RGPD. Ceci résulte du lien étroit entre d'une part l'article 5.2 du RGPD et d'autre part les obligations pour le responsable du traitement qui découlent des articles 24 et suivants du RGPD.

La Chambre Contentieuse renvoie à cet effet aux Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement 2016/679 du Groupe de travail Article 29 sur la protection des données[1] qui précisent ce qui suit :

"Qu'une violation doive être notifiée à l'autorité de contrôle ou non, le responsable du traitement est tenu de documenter toutes les violations, comme expliqué à l'article 33, paragraphe 5 :
Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.
Cette obligation de documentation est liée au principe de responsabilité du RGPD figurant à l'article 5, paragraphe 2. Cette exigence de tenir des registres des violations, qu'elles soient sujettes à notification ou non, est également liée aux obligations du responsable du traitement au titre de l'article 24, et l'autorité de contrôle peut demander à voir lesdits registres. Les responsables du traitement sont donc encouragés à établir un registre interne des violations, qu'ils soient tenus de les notifier ou non.
S'il appartient au responsable du traitement de déterminer la méthode et la structure à utiliser pour documenter une violation, certaines informations clés devraient être incluses en toutes circonstances. Comme requis à l'article 33, paragraphe 5, le responsable du traitement doit reprendre des informations concernant la violation, y compris les causes, les faits et les données à caractère personnel concernées. Il devrait également inclure les effets et les conséquences de la violation ainsi que les mesures prises par le responsable du traitement pour y remédier.
Le RGPD ne définit pas la période de conservation d'une telle documentation. Lorsque de tels registres contiennent des données à caractère personnel, il incombera au responsable du traitement de déterminer la période de conservation appropriée conformément aux principes liés au traitement de données à caractère personnel et au fondement juridique du traitement. Il devra conserver cette documentation conformément à l'article 33, paragraphe 5, dès lors que l'autorité de contrôle pourrait la réclamer à titre de preuve du respect dudit article, ou plus généralement du principe de responsabilité. De toute évidence, si les registres en eux-mêmes ne contiennent pas de données à caractère personnel, le principe de limitation de la conservation du RGPD ne s'applique pas.

[1] WP250.Rev01, pp 30-32.

Outre ces informations, le G29 recommande que le responsable du traitement documente également le raisonnement justifiant les décisions prises en réaction à la violation. En particulier, lorsqu'une violation n'est pas notifiée, la justification de cette décision devrait être documentée. Cette justification devrait inclure les raisons pour lesquelles le responsable du traitement considère que la violation est peu susceptible d'engendrer un risque pour les droits et libertés des individus. Si le responsable du traitement considère que l'une des conditions visées à l'article 34, paragraphe 3, est remplie, il devrait également pouvoir fournir des éléments de preuve appropriés à cet égard.

Lorsque le responsable du traitement ne notifie pas une violation à l'autorité de contrôle, mais que la notification est retardée, le responsable du traitement doit être en mesure de fournir les raisons d'un tel retard; une documentation à cet égard pourrait contribuer à démontrer que le retard de notification est bien justifié et n'est pas excessif.

Lorsque le responsable du traitement communique une violation aux personnes concernées, il devrait être transparent en ce qui concerne la violation en question et communiquer de façon efficace et en temps utile. Conserver la trace d'une telle communication aiderait ainsi le responsable du traitement à démontrer son respect du principe de responsabilité et du RGPD en général.

Dans le but de favoriser leur conformité avec les articles 33 et 34, il serait bénéfique à la fois pour les responsables du traitement et les sous-traitants de disposer d'une procédure de notification documentée définissant la procédure à suivre lorsqu'une violation est détectée, y compris concernant la façon d'endiguer, de gérer et de remédier à l'incident, d'évaluer le risque et de notifier la violation. À cet égard, toujours afin de prouver leur conformité avec le RGPD, il pourrait être utile de démontrer que les employés ont été informés de l'existence de tels mécanismes et procédures et qu'ils savent comment réagir en cas de violation.

Il convient de noter qu'en cas de manquement à cette obligation de documenter correctement une violation, l'autorité de contrôle pourrait exercer ses pouvoirs au titre de l'article 58 et/ou imposer une amende administrative conformément à l'article 83." [soulignement par la Chambre Contentieuse].

À la lumière des lignes directrices précitées, la Chambre Contentieuse a demandé au défendeur lors de l'audition dans quelle mesure il documentait les fuites de données.

Le défendeur a indiqué que toutes les fuites connues étaient documentées et que l'on faisait appel à cet effet à la loyauté et au professionnalisme du travailleur individuel afin de faire remonter au sein de l'entreprise une éventuelle fuite de données via l'outil disponible. Le défendeur affirme disposer des politiques nécessaires et organiser des formations afin de former ses travailleurs concernant la notification d'incidents liés aux données.

Vu ces explications fournies lors de l'audition, ainsi que le fait qu'il ressort des pièces du dossier que le défendeur, malgré sa contestation de la compétence de l'APD de réclamer des informations détaillées, a accédé à la demande de préciser le processus d'évaluation afin de permettre à l'APD de vérifier de quelle manière le défendeur est parvenu à une certaine conclusion en matière de risques dans un dossier concret, à savoir l'incident W, la Chambre Contentieuse doit conclure que le défendeur a exposé sa méthodologie et sa procédure en matière de violations et d'évaluation des risques.
La Chambre Contentieuse estime dès lors qu'on ne peut constater **aucune violation des articles 5.2, 24.1 et 33 du RGPD**.

d) Position du délégué à la protection des données (article 38 du RGPD)

Concernant la position du délégué à la protection des données, le rapport du Service d'Inspection établit les constatations suivantes :

Outre cette fonction, le délégué à la protection des données du défendeur remplit également la fonction de directeur audit, risk and compliance auprès du défendeur.

Il ressort de ce dossier que le délégué à la protection des données ne se trouve pas dans une position suffisamment protégée d'un conflit d'intérêts (comme l'impose l'article 38, paragraphe 6 du RGPD) et qu'il n'est pas suffisamment associé aux discussions relatives aux violations de données à caractère personnel (comme l'impose l'article 38, paragraphe 1 du RGPD).

Association insuffisante du délégué à la protection des données

- *Le délégué à la protection des données du défendeur est uniquement informé du résultat de l'évaluation des risques. À cet égard, nous nous référons au courrier du 12/06/2019 dans lequel la matrice RACI indique au point 1.4.2.2 que son délégué à la protection des données est uniquement "informed" et non "consulted". L'article 38, paragraphe 1 du RGPD requiert toutefois que le DPO soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.*
- *Les champs "avis du DPO " n'étaient jusqu'à récemment pas systématiquement complétés par le défendeur. Il ressort des explications reprises sous le point 1.4.2.2 du courrier du défendeur du 12/06/2019 (pièce 13) que la discussion relative au risque appartient au "business" (ce qui ressort également de la matrice RACI susmentionnée) et que jusqu'à récemment, l'avis du délégué à la protection des données n'était pas repris dans le formulaire type du défendeur ("Personal Data Breach Investigation Report").*

Conflit d'intérêts dans le chef du délégué à la protection des données

- *<u>Tâches conflictuelles.</u> Le défendeur affirme dans ses courriers du 03/04/2019 et du 12/06/2019 que son délégué à la protection des données a uniquement un rôle consultatif et*

ne peut pas prendre de décisions quant aux finalités et aux moyens du traitement, ce qui est également mentionné dans les [Lignes directrices concernant les délégués à la protection des données (DPD) du Groupe 29].[2] L'existence d'un conflit d'intérêts n'est toutefois pas limitée aux cas où une personne détermine les finalités et les moyens du traitement. Les conflits d'intérêts doivent toujours être évalués au cas par cas. Le courrier susmentionné du défendeur indique que son délégué à la protection des données fait plus que conseiller en interne le défendeur étant donné que cette personne effectue des tâches conflictuelles au sein d'Y (le défendeur) qui impliquent une responsabilité opérationnelle considérable pour les processus de traitement de données qui relèvent du domaine audit, risk et compliance.

- *Approche pragmatique en Allemagne et dans la doctrine,[3] qui [...] renvoient à des critères comme (1) l'existence ou non d'un auto-contrôle par un titulaire de la fonction qui fait autorité au sein de l'entreprise, (2) l'existence ou non de règles internes pour les conflits d'intérêts, et (3) assumer une responsabilité opérationnelle importante avec un impact sur les données à caractère personnel, ...*

- *Jusqu'il y a peu, le défendeur n'avait aucune politique visant à prévenir les conflits d'intérêts. Ce n'est qu'après les courriers recommandés de l'APD du 04/03/2019 et du 16/05/2019 remettant en cause la position du délégué à la protection des données qu'un document non daté "Y (défendeur) DPO Charter" a été transmis par courrier du défendeur du 12/06/2019, document qui devait encore être mis à l'ordre du jour du Comité Audit et Compliance en juillet 2019 (comme cela est mentionné en page 6 du courrier précité du défendeur). La rédaction d'un tel document n'implique pas qu'il soit ainsi suffisamment démontré que le délégué à la protection des données travaille de manière indépendante.*

Concernant l'**association du délégué à la protection des données**, il est souligné dans la défense que la constatation du Service d'Inspection est basée sur une mauvaise interprétation légale et factuelle.

Selon le défendeur, comme exposé dans ses conclusions, pour l'application de l'article 38.1 du RGPD, il suffirait que le délégué à la protection des données soit informé, ce qui constitue un élément de l'association, mais cette disposition n'impose pas l'obligation spécifique d'être consulté, contrairement à ce que mentionne le rapport d'inspection.

---

[2] WP 243Rev01, pp 20-21.

[3] Communiqué de presse de l'autorité de contrôle bavaroise du 20/10/2016 sur un manager IT, publié sur le lien suivant : https://www.lda.bayern.de/media/pm2016 OS.pdf et commenté sur le lien suivant : https://iapp.org/news/a/german-company-fined-for-dpo-conflict-of-interest/ ainsi que la doctrine en la matière (à savoir F. SCHRAM, De functionaris voor gegevensbescherming, Édition Cahier 2, Politeia, 2019, 119-121).

La Chambre Contentieuse estime que le point de vue du défendeur n'est pas conforme à la *ratio legis* et n'est pas une interprétation sensée de l'article 38.1 du RGPD qui dispose que le délégué doit être "*associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel*". Réduire l'association du délégué à la protection des données à sa simple information (a posteriori) concernant une décision vide sa fonction de son contenu.

À cet égard, la Chambre Contentieuse renvoie en particulier aux Lignes directrices du Groupe 29 pour les délégués à la protection des données[4], qui soulignent qu'il est essentiel que le délégué à la protection des données soit associé dès le stade le plus précoce possible à toutes les questions relatives à la protection des données. Veiller à ce que le délégué à la protection des données soit informé et, plus important encore, consulté dès le début permet de respecter le Règlement général sur la protection des données.

En outre, cela favorise le respect d'une approche de la protection des données dès la conception, telle que prévue à l'article 25 du RGPD et qui doit dès lors être la procédure habituelle au sein de la gouvernance de l'organisme.

La Chambre Contentieuse constate que le défendeur a mal interprété l'article 38.1 du RGPD. Toutefois, la Chambre Contentieuse estime qu'il est rendu suffisamment plausible qu'en ce qui concerne le *processus d'évaluation des risques*, le délégué à la protection des données soit associé dans la pratique et mène lui-même une analyse indépendante des risques en matière de vie privée, avant la décision finale sur les risques, au moyen d'un avis et de son assistance en tant que conseiller.

Concernant le *résultat de l'évaluation des risques*, selon lequel une décision finale a été prise par les représentants au sein de l'équipe ou du département responsable des services ou clients affectés, le délégué à la protection des données est uniquement informé, pas consulté. Cela est conforme à l'article 38.1 du RGPD combiné à l'article 39.1.a) du RGPD qui exige que le délégué à la protection des données ait un rôle consultatif à l'égard du responsable du traitement, mais ne soit pas coresponsable de la décision finale. Sur cette base, la Chambre Contentieuse confirme que le délégué à la protection des données est uniquement informé de la décision finale relative aux risques.

[4] "*Il est essentiel que le DPD, ou son équipe, soit associé dès le stade le plus précoce possible à toutes les questions relatives à la protection des données. En ce qui concerne les analyses d'impact relatives à la protection des données, le RGPD prévoit expressément la participation du DPD à un stade précoce et précise que le responsable du traitement doit demander conseil au DPD lorsqu'il effectue une analyse de ce type. L'information et la consultation du DPD dès le début permettront de faciliter le respect du RGPD et d'encourager une approche fondée sur la protection des données dès la conception; il devrait donc s'agir d'une procédure habituelle au sein de la gouvernance de l'organisme. En outre, il importe que le DPD soit considéré comme un interlocuteur au sein de l'organisme et qu'il soit membre des groupes de travail consacrés aux activités de traitement de données au sein de l'organisme.*", WP24301Rev, paragraphe 3.1 des lignes directrices, soulignement par la Chambre Contentieuse.

La Chambre Contentieuse conclut que d'une part, le défendeur a une interprétation erronée de la position du délégué à la protection des données mais que d'autre part, il est plausible que dans la pratique, le délégué à la protection des données soit suffisamment associé. Dès lors, **aucune violation de l'article 38.1 du RGPD** ne peut être constatée.

En ce qui concerne la constatation du Service d'Inspection selon laquelle il y a un **conflit d'intérêts** dans le chef du délégué à la protection des données en raison du fait qu'il est également responsable de la gestion de la conformité et des risques et de l'audit interne, le défendeur avance que dans l'exercice de chacune de ces fonctions, la personne concernée ne prend elle-même aucune décision mais que son rôle est purement consultatif. En outre, les mesures nécessaires auraient été prises en interne pour éviter le risque de conflit d'intérêts. Ces mesures ont été formalisées dans une DPO Charter qui a été validée par le comité d'audit du défendeur le 29 juillet 2019.

Lors de l'audition, la Chambre Contentieuse a examiné l'impact que le délégué à la protection des données a sur le processus décisionnel en raison de ses autres fonctions. Concernant le rôle du délégué à la protection des données, la Chambre Contentieuse soulève la question de savoir comment cette fonction est compatible avec celle consistant à réaliser des audits internes dans le cadre desquels certains éléments pouvant, le cas échéant, donner lieu au licenciement d'un travailleur déterminé peuvent être établis dans un rapport. Dans ce cadre, il importe de savoir si le délégué à la protection des données qui endosse également la fonction de chef de l'audit interne a également un droit de décision en cette qualité.

La Chambre Contentieuse souligne qu'il existe une différence entre la simple analyse de processus et l'évaluation du fonctionnement des travailleurs via un audit interne, ce qui est en contradiction avec la fonction de confiance que le délégué à la protection des données a au sein de l'entreprise. À cet égard, le défendeur affirme qu'aucun problème de compatibilité ne se pose étant donné qu'en tant que chef de l'audit interne, le délégué à la protection des données concerné ne prend aucune décision individuelle concernant les travailleurs et ne les évalue pas non plus.

La Chambre Contentieuse constate que dans ses conclusions, le défendeur aborde en détail l'indépendance et le rôle consultatif de chacun des trois départements, à savoir le département Compliance, le département Audit interne et le département Risk Management, à l'égard des autres sections de l'entreprise. Ainsi, le défendeur précise que les rôles Audit, Compliance et Risk n'impliquent que des risques limités de conflits d'intérêts car ils ont des fonctions "consultatives" et n'ont pas de compétence de décision concernant les activités de traitement. Cela conduit le défendeur à affirmer que le délégué à la protection des données n'a aucune tâche (même pas via ses fonctions dans chacun

des départements) où il pourrait prendre des décisions quant aux finalités et aux moyens du moindre traitement de données à caractère personnel. [5]

La Chambre Contentieuse estime qu'il n'est pas démontré ainsi que le délégué à la protection des données, qui fait partie de chacun de ces départements et y endosse une position à responsabilités, n'exerce aucune tâche qui soit incompatible avec sa position en tant que délégué à la protection des données.

La Chambre Contentieuse fait donc remarquer que l'indépendance et le rôle consultatif du département en tant que tel ne peuvent pas être appliqués sans condition à la personne qui remplit simultanément la fonction de délégué à la protection des données et de responsable d'un département.

La Chambre Contentieuse doit évaluer de quelle manière et dans quelle mesure l'indépendance du délégué à la protection des données est assurée vis-à-vis de chacun de ces trois départements, en particulier dans une situation comme le cas présent où le délégué à la protection des données fait non seulement partie de ces départements mais assure également le rôle de responsable de ces départements.

En effet, le défendeur stipule explicitement qu'outre les responsabilités en tant que délégué à la protection des données, la même personne est également responsable de la compliance, du risk management et de l'audit interne.[6] Le défendeur désigne donc lui-même une même personne physique en tant que responsable de chacun des trois départements et en tant que délégué à la protection des données. Cette responsabilité pour chacun de ces trois départements implique incontestablement que cette personne, en cette qualité, détermine les finalités et les moyens du traitement de données à caractère personnel au sein de ces trois départements et donc est responsable des processus de traitement de données qui relèvent du domaine de la compliance, du risk management et de l'audit interne, comme cela a été constaté dans le rapport d'inspection.

Les Lignes directrices du Groupe 29 concernant les délégués à la protection des données[7] expliquent que le délégué à la protection des données ne peut exercer au sein de l'organisme une fonction qui

---

[5] Conclusions du défendeur, n° 166 et 167.

[6] Voir la lettre du 3 avril 2019 à l'APD, citée dans les conclusions.

[7] "*L'article 38, paragraphe 6, autorise les DPD à "exécuter d'autres missions et tâches". Il exige toutefois que l'organisme veille à ce que "ces missions et tâches n'entraînent pas de conflit d'intérêts".*
L'absence de conflit d'intérêts est étroitement liée à l'obligation d'agir en toute indépendance. Bien que les DPD soient autorisés à exercer d'autres fonctions, un DPD ne peut se voir confier d'autres missions et tâches qu'à condition que celles-ci ne donnent pas lieu à un conflit d'intérêts. Cela signifie en particulier que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. En raison de la structure organisationnelle spécifique de chaque organisme, cet aspect doit être étudié au cas par cas.
En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent

l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. Il s'agit donc d'un conflit d'intérêts substantiel. Le rôle de responsable d'un département n'est donc pas conciliable avec la fonction de délégué à la protection des données qui doit pouvoir exercer ses tâches en toute indépendance. Le cumul, dans le chef d'une même personne physique, de la fonction de responsable de chacun des trois départements en question distinctement d'une part et de la fonction de délégué à la protection des données d'autre part prive chacun de ces trois départements de toute possibilité de contrôle indépendant par le délégué à la protection des données. En outre, le cumul de ces fonctions peut avoir pour effet que le secret et la confidentialité envers les membres du personnel ne puissent pas être suffisamment garantis, conformément à l'article 38.5 du RGPD. La Chambre Contentieuse estime dès lors que la **violation de l'article 38.6 du RGPD** est avérée.

Il importe que le délégué à la protection des données puisse exécuter ses missions et tâches dans le respect de la position telle que l'article 38 du RGPD la lui a attribuée, en particulier qu'il puisse intervenir sans qu'il y ait conflit d'intérêts. La Chambre Contentieuse charge donc le défendeur de mettre le traitement en conformité avec l'article 38.6 du RGPD sur ce point et ainsi de veiller à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts.

Compte tenu du fait que le RGPD a confié un rôle-clé au délégué à la protection des données en lui attribuant une mission informative et consultative à l'égard du responsable du traitement concernant toutes les questions relatives à la protection des données à caractère personnel, dont la notification de violations de données, la Chambre Contentieuse procède également à l'imposition d'une amende administrative.

Outre la mesure correctrice visant à mettre le traitement en conformité avec l'article 38.6 du RGPD, la Chambre Contentieuse décide également d'infliger une amende administrative dont le but n'est pas de mettre fin à une infraction commise mais bien de faire appliquer efficacement les règles du RGPD. Comme cela ressort du considérant 148, le RGPD souhaite que des sanctions, y compris des amendes administratives, soient infligées en cas de violations sérieuses, en complément ou à la place des

---

la détermination des finalités et des moyens du traitement. En outre, il peut également y avoir conflit d'intérêts, par exemple, si un DPD externe est appelé à représenter le responsable du traitement ou le sous-traitant devant les tribunaux dans des affaires ayant trait à des questions liées à la protection des données.
En fonction des activités, de la taille et de la structure de l'organisme, il peut être de bonne pratique pour les responsables du traitement ou les sous-traitants :

- *de recenser les fonctions qui seraient incompatibles avec celle de DPD ;*
- *d'établir des règles internes à cet effet, afin d'éviter les conflits d'intérêts ;*
- *d'inclure une explication plus générale concernant les conflits d'intérêts ;*
- *de déclarer que leur DPD n'a pas de conflit d'intérêts en ce qui concerne sa fonction de DPD, dans le but de mieux faire connaître cette exigence ;*
- *de prévoir des garanties dans le règlement intérieur de l'organisme, et de veiller à ce que l'avis de vacance pour la fonction de DPD ou le contrat de service soit suffisamment précis et détaillé pour éviter tout conflit d'intérêts. Dans ce contexte, il convient également de garder à l'esprit que les conflits d'intérêts peuvent prendre différentes formes selon que le DPD est recruté en interne ou à l'extérieur.*"

WP243Rev01, paragraphe 3.5, soulignement par la Chambre Contentieuse.

mesures appropriées qui sont imposées[8]. La Chambre Contentieuse agit ainsi en application de l'article 58.2.i) du RGPD. L'instrument de l'amende administrative n'a donc nullement pour but de mettre fin aux violations. À cet effet, le RGPD et la LCA prévoient plusieurs mesures correctrices, dont les ordres cités à l'article 100, § 1er, 8° et 9° de la LCA.

Tout d'abord, la nature et la gravité de la violation sont prises en considération par la Chambre Contentieuse afin de justifier l'imposition de cette sanction et l'ampleur de celle-ci.

Dans ce cadre, la Chambre Contentieuse constate que bien qu'il n'y ait aucun élément révélant qu'il soit question d'une violation intentionnelle, il s'agit d'un manquement grave dans le chef du défendeur. Bien que le délégué à la protection des données soit une fonction prescrite obligatoirement pour la première fois au niveau européen dans le RGPD, le concept d'un délégué à la protection des données n'est pas nouveau et existe depuis longtemps dans de nombreux États membres et dans de nombreuses organisations.[9]

En outre, le Groupe 29 a déjà établi des lignes directrices pour ces délégués le 13 décembre 2016. Ces lignes directrices ont été revues le 5 avril 2017 après une large consultation publique. Comme il ressort de ce qui précède, ces lignes directrices sont claires concernant la mesure dans laquelle le délégué à la protection des données peut également remplir d'autres fonctions au sein de l'entreprise, en tenant compte de la structure organisationnelle propre à chaque organisme et cet aspect doit être étudié au cas par cas.

En bref, selon la Chambre Contentieuse, il n'existe aucun doute quant au fait que le cumul de la fonction de délégué à la protection des données avec une fonction en tant que chef d'un département que le délégué à la protection des données doit contrôler ne peut pas avoir lieu de manière indépendante.

On peut attendre d'une organisation telle que le défendeur qu'elle se prépare consciencieusement à l'introduction du RGPD et ce dès l'entrée en vigueur du RGPD, conformément à l'article 99 du RGPD en mai 2016. Le traitement de données à caractère personnel constitue en effet une activité essentielle

---

[8] Le considérant 148 dispose ce qui suit : "*Afin de renforcer l'application des règles du présent règlement, des sanctions y compris des amendes administratives devraient être infligées pour toute violation du présent règlement, en complément ou à la place des mesures appropriées imposées par l'autorité de contrôle en vertu du présent règlement. En cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende. Il convient toutefois de tenir dûment compte de la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant, de l'application d'un code de conduite, et de toute autre circonstance aggravante ou atténuante. L'application de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la Charte, y compris le droit à une protection juridictionnelle effective et à une procédure régulière.*"

[9] Voir notamment WP243Rev01, paragraphe 1.

du défendeur, qui traite en outre des données à caractère personnel à très grande échelle, dont des données à caractère personnel qui peuvent présenter un caractère très sensible, notamment parce qu'elles permettent une observation régulière et systématique.[10]

La durée de l'infraction est également prise en considération. Le délégué à la protection des données a été créé par le RGPD, qui s'applique depuis le 25 mai 2018, de sorte que la violation de l'article 38.6 du RGPD est déjà établie à partir de cette date. Quoi qu'il en soit, l'infraction persistait encore à la date de l'audition, c'est-à-dire le 14 février 2020.

Enfin, le défendeur traite des données à caractère personnel de millions de personnes. Des garanties inefficaces pour la protection des données à caractère personnel, plus précisément en désignant un délégué à la protection des données qui ne répond pas à l'exigence d'indépendance et ne peut donc pas intervenir sans conflit d'intérêts, ont donc un impact potentiel sur des millions de personnes concernées.

L'ensemble des éléments exposés ci-dessus justifie une sanction effective, proportionnée et dissuasive, telle que visée à l'article 83 du RGPD, compte tenu des critères d'appréciation qu'il contient, à concurrence d'un montant de 50.000 euros. La Chambre Contentieuse attire l'attention sur le fait que les autres critères de l'article 83.2 du RGPD ne sont pas, dans ce cas, de nature à conduire à une autre amende administrative que celle définie par la Chambre Contentieuse dans le cadre de la présente décision.

e) Publication de la décision

Vu l'importance de la transparence concernant le processus décisionnel de la Chambre Contentieuse, la présente décision est publiée sur le site Internet de l'Autorité de protection des données. Toutefois, il n'est pas nécessaire à cette fin que les données d'identification des parties soient directement communiquées.

PAR CES MOTIFS,

la Chambre Contentieuse de l'Autorité de protection des données décide, après délibération :
- en vertu de l'article 100, § 1er, 9° de la LCA, d'**ordonner au défendeur que le traitement soit mis en conformité** avec l'article 38.6 du RGPD. À cet effet, la Chambre Contentieuse accorde au

[10] Voir notamment l'article 37.1 du RGPD. Voir à cet égard également la jurisprudence de la Cour européenne de justice concernant le caractère potentiellement sensible des données de télécommunication, comme par ex. les affaires jointes C-293/12 et C-594/12, Digital Rights Ireland et Seitlinger e.a., ECLI:EU:C:2014:238, paragraphe 37.

défendeur un délai de trois mois et attend du défendeur qu'il lui fasse rapport au plus tard le 31 juillet 2020 concernant la mise en conformité du traitement avec les dispositions susmentionnées ;
- en vertu de l'article 100, § 1er, 13° de la LCA et de l'article 101 de la LCA d'infliger **une amende administrative** de 50.000 euros.

En vertu de l'article 108, § 1er de la LCA, cette décision peut faire l'objet d'un recours dans un délai de trente jours, à compter de la notification, à la Cour des marchés, avec l'Autorité de protection des données comme défendeur.

(sé.) Hielke Hijmans
Président de la Chambre Contentieuse