NIVEAU 2

CONCEPTION : PROCEDURES, ROUTINES ET DOCUMENTS RGPD

Mots clés : badge, chèque de repas, consentement, données personnelles des employés, droit d'accès, droit d'effacement, géolocalisation, images, photos, transparence, vidéosurveillance

MAITRISEZ LA « TRANSPARENCE »

Illustration : Données personnelles des employés

1. Le traitement de données personnelles des employés

Depuis le processus de recrutement et après la fin de la relation de travail, l'employeur se trouve confronté à un nombre important de cas où il devra appliquer les règles relatives à la protection des données.

En effet, un employeur est souvent amené à collecter des données à caractère personnel, par exemple lorsqu'un candidat lui envoie son dossier de candidature, lorsqu'un salarié lui communique ses coordonnées bancaires pour qu'il puisse procéder au paiement de son salaire, lors des évaluations professionnelles annuelles de ses salariés, ou encore afin de rembourser des frais de route à un de ses salariés.

Il appartient à l'employeur de déterminer, avant tout traitement de données personnelles et au regard du contexte spécifique, quelle(s) base(s) de licéité est (sont) le(s) plus appropriée(s) et pourrai(en)t justifier le traitement envisagé.

Il revient encore à l'employeur, en qualité de responsable du traitement (voir encart « *Bon à savoir* ») de documenter sa conformité au RGPD (principe d'« accountability » ou de responsabilisation). Cette documentation sera nécessaire pour le responsable du traitement, notamment en cas de contrôle par la CNPD ou quand les personnes concernées font usage de leurs droits (voir infra).

Les catégories particulières de données (« données sensibles ») :

Une vigilance particulière est nécessaire en cas de traitement de données dites « sensibles ». Il s'agit des catégories particulières de données au sens de l'article 9 du RGPD, à savoir des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé

BON A SAVOIR

Responsable du traitement

Dans le cadre de la relation du travail, le responsable du traitement est en principe l'employeur. Ainsi, un membre du personnel ou un département spécifique ne sera en principe pas le responsable du traitement, mais agira au nom de l'employeur, qui est responsable du respect du RGPD.

Bon à savoir : La délégation du personnel, en tant qu'organe représentatif des salariés, est à considérer comme étant distincte de l'employeur et donc un responsable du traitement à part.

Sous-traitant

Bon à savoir : Un sous-traitant ne peut pas traiter les données qui lui ont été confiées par un responsable de traitement à ses propres fins. Autrement, il devient le responsable des traitements ainsi effectués, avec toutes les responsabilités qui s'y attachent.

Bon à savoir : Les parties ne peuvent pas convenir librement dans le contrat de leurs qualités respectives sous le RGPD. Les qualifications de responsable de traitement ou de sous-traitant doivent découler d'une analyse factuelle, et ce pour chaque traitement de données.

ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Par exemple, l'information qu'une salariée est en congé de maternité est à considérer comme une donnée « sensible », car cette information est une donnée relative à la santé de la personne concernée. Il en est de même pour le certificat médical d'embauche, qui, du fait qu'il informe l'employeur de l'aptitude ou non d'un salarié pour un poste donné, contient des données relatives à la santé du salarié.

De même, l'information selon laquelle un salarié est membre d'un syndicat constitue une « donnée sensible ».

2. Obligation de transparence

Conformément aux principes de transparence et de loyauté, les personnes concernées (par exemple, les candidats et les salariés) doivent recevoir certaines informations concernant le traitement de leurs données par l'employeur, afin de leur permettre de comprendre pourquoi les données sont collectées, l'usage qui en sera fait ainsi que les droits dont elles disposent pour contrôler la licéité des traitements effectués par l'employeur.

BON A SAVOIR:

Conformément au principe de responsabilisation, l'employeur doit à tout moment pouvoir démontrer qu'il a bien fourni les informations requises aux personnes concernées.

L'employeur devrait également prendre en compte d'éventuelles obligations sectorielles ou découlant d'autres législations, telles que l'obligation d'information concernant la surveillance sur le lieu de travail découlant de l'article L. 261-1 du Code du travail.

Les caractéristiques de l'information à donner

Tout responsable du traitement est obligé d'informer individuellement les personnes concernées du traitement de données à caractère personnel qu'il met en œuvre.

Conformément à l'article 12.1 du RGPD, la fourniture d'informations aux personnes concernées et les communications qui leur sont adressées doivent être réalisées d'une façon « concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ».

Le mot « fournir » est crucial en l'occurrence et il signifie que le responsable du traitement doit prendre des mesures concrètes pour transmettre les informations en question à la personne concernée ou pour diriger activement la personne concernée vers l'emplacement desdites informations (par exemple au moyen d'un lien direct, d'un code QR, etc.).

Le contenu de l'information

L'employeur doit fournir aux salariés toutes les informations listées à l'article 13 du RGPD (ou l'article 14, si les données ne sont pas collectées directement auprès de la personne concernée), dans les conditions prévues par les articles 12, 13 et 14 du RGPD.

Les informations à fournir doivent permettre aux personnes concernées de comprendre l'envergure des traitements effectués par l'employeur et doivent être adaptées aux spécificités desdits traitements. L'employeur doit, entre autres, indiquer :

- les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement (à savoir la condition de licéité sur laquelle repose(nt) le(s) traitement(s) ; si des données dites « sensibles » sont traitées, l'exception de l'article 9 du RGPD qui s'applique, et si les données judiciaires au sens de l'article 10 du RGPD sont traitées, les dispositions légales en vertu duquel le traitement est effectué ;
- lorsque le traitement est fondé sur l'intérêt légitime, une description des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;
- lorsque les données sont collectées directement auprès de la personne concernée, si l'exigence de fournir les données personnelles à un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données (p.ex. le numéro d'identification national) ;

- lorsque les données ne sont pas collectées directement auprès de la personne concernée, la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public (p.ex. un réseau social).

La CNPD recommande aux employeurs de s'assurer que les traitements de données repris dans la notice d'information correspondent bien aux traitements répertoriés dans le registre des traitements.

Sous quelle forme faut-il fournir les informations ?

Les informations et les communications devraient, en principe, être adressées aux personnes concernées par écrit. Elles peuvent également être accompagnées par d'autres moyens afin de faciliter la compréhension des personnes concernées.

Par ailleurs, le RGPD exige que les informations soient « fournies » aux personnes concernées.

L'employeur pourrait par exemple satisfaire à son obligation d'information en fournissant les informations requises dans une annexe au contrat de travail ou en insérant dans les contrats de travail une clause relative aux traitements de données personnelles effectués dans le cadre de la gestion du personnel pour autant que la clause en question soit claire, complète, explicite et soit clairement différenciée des autres termes du contrat.

BON A SAVOIR:

Il y a lieu de souligner dans ce contexte que la simple signature d'une fiche d'information ou du contrat de travail par le salarié peut tout au plus être considérée comme un accusé de réception permettant à l'employeur de documenter qu'il a bien fourni les informations requises au salarié, mais ne peut en aucun cas valoir consentement valide du salarié au traitement de données par son employeur au sens du RGPD.

Les modalités de fourniture et de présentation de cette information doivent être adaptées aux circonstances de la collecte et du traitement des données et doivent notamment permettre aux personnes concernées de comprendre la raison de la collecte des différentes données les concernant, le traitement qui en sera fait ainsi que leurs droits. Ainsi, en fonction des conditions du traitement, il pourrait être utile pour le responsable du traitement d'adopter une approche à plusieurs niveaux pour la communication des informations aux personnes concernées.

Le premier niveau d'information devrait inclure les informations les plus importantes, à savoir les détails de la finalité du traitement, l'identité du responsable du traitement, une description des droits des personnes concernées et une référence obligatoire vers le deuxième niveau d'information où les personnes concernées peuvent trouver toutes les informations, par exemple au moyen d'un code QR ou d'un lien direct. En fonction du traitement, l'employeur devrait également inclure dans le premier niveau des informations sur le traitement qui aura la plus forte incidence sur la personne concernée et sur tout traitement qui pourrait la surprendre. Aussi la personne concernée devrait-elle être en mesure de comprendre à partir des informations fournies au premier niveau/à la première modalité quelles seront pour elle les conséquences du traitement en question.

BON A SAVOIR:

Un simple renvoi au RGPD n'est pas conforme aux exigences du RGPD en matière de transparence. L'employeur doit fournir des informations spécifiques concernant les traitements qu'il effectue.

Conformément au principe de responsabilisation, il ne relève pas des missions de la CNPD d'analyser ou de valider a priori la notice d'information de l'employeur.

Exemple

Afin de protéger les biens de l'entreprise et sécuriser l'accès au bâtiment, l'employeur souhaite installer un système de vidéosurveillance pour surveiller les locaux où travaillent ses salariés. Il installe à la porte d'entrée principale du bâtiment un pictogramme doté de la mention « surveillance vidéo 24h/24h » et il en informe également la délégation du personnel.

En l'espèce, l'employeur n'a pas respecté les exigences d'information imposées par l'article 13 du RGPD. En effet, la simple information de la délégation du personnel n'assure pas que les salariés aient été informés individuellement des éléments précis de l'article 13 du RGPD. Par ailleurs, le pictogramme mentionnant une « surveillance vidéo 24h/24h » ne contient pas tous les éléments requis.

Dans ce contexte du traitement des données personnelles au moyen d'un système de vidéosurveillance, l'employeur pourrait utiliser deux niveaux d'information. Le premier niveau devrait de manière générale inclure les informations les plus essentielles (les détails de la finalité du traitement, l'identité du responsable du traitement, l'existence des droits des personnes concernées et une référence obligatoire vers le deuxième niveau d'information, par exemple au moyen d'un code QR ou d'un lien direct). La CNPD met à disposition sur son site internet un modèle de panneau d'affichage de premier niveau.

Le deuxième niveau d'information, c'est-à-dire l'ensemble des informations requises au titre de l'article 13 du RGPD pourrait être fourni par d'autres moyens, comme par exemple un exemplaire de la politique de confidentialité envoyé par courriel à tous les salariés.

A quel moment faut-il fournir les informations ?

Le moment de la communication des informations dépend de la forme de la collecte. Or, peu importe la forme de la collecte, la communication rapide des informations « … est un élément essentiel de l'obligation de transparence et de l'obligation de traiter les données avec équité. »

En cas de collecte directe, les informations doivent être fournies au plus tard au moment de la collecte auprès de la personne concernée, par exemple lorsqu'un candidat remplit un formulaire mis à disposition par l'employeur. L'employeur doit donc s'assurer que le (futur) salarié ait reçu les informations requises dès que les données sont collectées

En cas de collecte indirecte, les informations doivent être fournies dès que possible (notamment lors du premier contact avec la personne concernée), sauf exceptions.

L'employeur devrait documenter la fourniture des informations à des fins de preuve comme par exemple par la signature d'un récépissé certifiant la remise des informations.

Pour en savoir plus : Article 12, 13 et 14 du RGPD, Fiche pratique et vidéoclip de la CNPD sur le droit à l'information.

QUELQUES « ROUTINES » RGPD DU MONDE PROFESSIONNEL

1. La vidéosurveillance

Finalité

Conformément à l'article 5.1, b) du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

A titre d'exemple, la surveillance par caméras vidéo peut avoir pour finalités :

- de sécuriser les accès au bâtiment ;
- d'assurer la sécurité du personnel et des clients ;
- de détecter et d'identifier des comportements potentiellement suspects ou dangereux susceptibles de provoquer des accidents ou incidents ;
- de repérer avec précision l'origine d'un incident ;
- de protéger les biens (bâtiments, installations, matériel, marchandes, liquidités, etc.) ;
- d'organiser et d'encadrer une évacuation rapide des personnes en cas d'incident ;
- de pouvoir alerter en temps utile les services de secours, d'incendie ou des forces de l'ordre ainsi que de faciliter leur intervention.

Avant l'installation d'un système de vidéosurveillance, le responsable du traitement devra définir, de manière précise, la ou les finalités qu'il souhaite atteindre en recourant à un tel système, et ne pourra pas l'utiliser ensuite à d'autres fins.

Protection des biens et comportements des employés

La CNPD estime que la vidéosurveillance ne doit pas servir à observer le comportement et les performances des membres du personnel du responsable du

traitement en dehors des finalités pour lesquelles elle a été mise en place.

Ainsi, un employeur a le droit d'utiliser les images d'un salarié commettant un vol de marchandises et qui proviennent d'un système de vidéosurveillance utilisé pour une finalité de protection des biens. Or, il n'a pas le droit de prendre des mesures à l'encontre d'un salarié lorsque, au goût de l'employeur, le salarié discute trop longtemps avec un client ou un collègue de travail et que ce comportement est enregistré par le système de vidéosurveillance. Ceci constituerait un détournement de finalité interdit par le RGPD.

Exemple : caisse d'un magasin

La surveillance par caméra d'une caisse d'un magasin peut avoir pour finalités de protéger les biens du responsable du traitement contre les actes de vol commis par ses salariés ou par un client/usager et d'assurer la sécurité de son personnel. Toutefois, afin de ne pas porter atteinte à la vie privée des salariés, la caméra devra être configurée de façon à ce que les salariés présents derrière un comptoir-caisse ne soient pas ciblés, en orientant son champ de vision vers la caisse elle-même et l'avant du comptoir, c'est-à-dire l'espace d'attente des clients se trouvant devant le comptoir, et ce, en vue de permettre l'identification des auteurs d'agressions, par exemple.

Exemple : lieu d'accès

Les caméras destinées à surveiller un lieu d'accès (entrée et sortie, seuil, perron, porte, auvent, hall, etc.) doivent avoir un champ de vision limité à la surface strictement nécessaire pour visualiser les personnes s'apprêtant à y accéder ; celles qui filment des accès extérieurs ne doivent pas baliser toute la largeur d'un trottoir longeant, le cas échéant, le bâtiment ou les voies publiques adjacentes. De même, les caméras extérieures installées aux abords ou alentours d'un bâtiment doivent être configurées de façon à ne pas capter la voie publique, ni les abords, entrées, accès et intérieurs d'autres bâtiments avoisinants rentrant éventuellement dans leur champ de vision. En fonction de la configuration des lieux, il est parfois impossible d'installer une caméra qui ne comprendrait pas dans son champ de vision une partie de la voie publique, abords, entrées, accès et intérieurs d'autres bâtiments. Dans un tel cas, la CNPD estime que le responsable du traitement doit mettre en place des techniques de masquages ou de floutage afin de limiter le champ de vision à sa propriété.

Pour en savoir plus : Lignes directrices vidéosurveillance publiées sur le site de la CNPD

2. Le dispositif de badge

Le RGPD n'interdit pas l'affichage des noms et prénoms sur des badges, mais exige que des mesures appropriées soient mises en place vis-à-vis de ces données personnelles.

Les principes de minimisation des données et de proportionnalité doivent être pris en compte lors de la création des badges, en veillant à ce que seules les informations strictement nécessaires à l'objectif poursuivi soient affichées.

Par exemple, afficher uniquement le prénom, recourir à l'utilisation de codes ou encore d'initiales peuvent être des mesures efficaces pour protéger la vie privée des individus tout en permettant leur identification lorsqu'il est nécessaire.

En ce qui concerne la photographie, dans certains cas de figure, l'employeur peut exiger qu'une photo soit prise pour la confection d'un badge d'accès nécessaire pour des raisons de sécurité. Il n'est en revanche pas admis d'exiger la publication d'une photo sur un réseau interne, sur internet ou dans une publication papier.

BON A SAVOIR:

La photo prise pour la confection d'un badge d'accès ou de légitimation (photo imprimée sur le badge pour qu'une identification visuelle soit possible) ne peut pas automatiquement être réutilisée pour l'organigramme interne ou la messagerie interne.

3. Le chèque de repas

Le règlement grand-ducal modifié du 29 décembre 1986 portant exécution de l'article 115, numéro 21 de la loi concernant l'impôt sur le revenu prévoit dans ce contexte en son article 2, paragraphe (2) que « les chèques de repas doivent, en dehors de la désignation de l'employeur émetteur, de leur valeur et de leur objet, porter un signe distinctif permettant d'en identifier l'utilisateur. »

Dans ce contexte, la CNPD considère que l'utilisation du numéro d'identification national (dit « matricule ») pour la finalité d'émettre des chèques repas (digitalisés ou non) apparaît comme incompatible avec le principe de la minimisation des données.

4. L'image et la prise de photos

En matière de droit à l'image, il est de jurisprudence constante que « toute personne a sur son image et l'utilisation qui en est faite un droit exclusif et peut s'opposer à une diffusion non autorisée par elle ». Ainsi, « chacun peut s'opposer à la publication de ses traits sans autorisation ».

Comme le consentement en matière de protection des données, le consentement en terme de droit à l'image doit être libre, certain et spécifique. Cela signifie qu'en principe, l'employé doit pouvoir s'opposer ou consentir de façon distinct à la prise de vue ou à la transmission d'une image, et à la diffusion sur les différents supports de publication (site internet, réseau interne, supports papier). L'employé garde la maîtrise de son image et il peut en principe refuser une « prise de photos intempestive et au pied levé » et aussi retirer son consentement pour la publication d'une photo spécifique.

Cependant, une donnée à caractère personnel étant toute information se rapportant à une personne physique identifiée ou identifiable, une photographie est donc une donnée personnelle.

Ainsi, en matière de protection des données personnelles, une des conditions à remplir pour que le consentement soit valable – qui découlent de l'article 4. 11) du RGPD – est que celui-ci ait été donné librement par la personne concernée. Or, étant donné la dépendance et le déséquilibre de pouvoirs qui peuvent exister dans les relations « employeur-salarié », les salariés ne sont que très rarement en mesure de pouvoir refuser ou révoquer leur consentement sans craindre d'en subir des conséquences défavorables. Dans ces conditions, le consentement ne peut être considéré comme étant donné librement.

Enfin, la divulgation des données à caractère personnel telles qu'une photo dans un réseau interne aux employés ne semble pas conforme au principe de minimisation des données énoncé à l'article 5.1, point c), du RGPD. Par conséquent, la photographie de l'employé ne semble pas nécessaire dans la plupart des contextes de travail au regard de l'objectif de mise en place d'un réseau interne.

Pour résumer : En dehors de certains cas précis, la majorité des relations de travail ne justifient pas de récolter la photographie des employés pour les introduire dans la messagerie interne de l'entreprise.

Pour en savoir plus : Lignes directrices « droit à l'image » publiées sur le site de la CNPD

5. La géolocalisation

Base légale

Tout traitement de données à caractère personnel doit reposer sur une des conditions de licéité limitativement énumérées à l'article 6.1 3 du RGPD. Dans le cadre d'un dispositif de géolocalisation mis en place par un employeur à l'égard de ses salariés, une condition de licéité valable pourrait être que le traitement est nécessaire aux fins des intérêts légitimes du responsable de traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la ou des personne(s) géolocalisée(s) (article 6.1, f) du RGPD).

Par ailleurs, dans le cas où l'installation d'un dispositif de géolocalisation des véhicules des salariés est imposée à l'employeur par une règle de droit national ou européen (p.ex. législation applicable dans le domaine du transport routier national et international), la condition de licéité de l'article 6.1, c) du RGPD pourrait s'appliquer.

Pour les raisons expliquées *supra* (encart sur le caractère libre du consentement), le consentement ne constitue pas une base de licéité appropriée en matière de géolocalisation des salariés.

Horaires de travail

Les systèmes de géolocalisation des véhicules mis à la disposition des salariés permettent aux employeurs de suivre les déplacements de leurs salariés dans le temps et dans l'espace. La démocratisation de ces systèmes rend leur utilisation de plus en plus fréquente dans le monde de l'entreprise. Cependant, comme l'utilisation de ces dispositifs implique un traitement de données à caractère personnel, il pose certaines questions de protection des données et comporte des risques pour la vie privée des salariés. **Ainsi, la géolocalisation expose**

les salariés au risque d'être suivis en temps réel par leur employeur en dehors des périodes de travail, ou encore au risque que le système de géolocalisation soit utilisé par l'employeur pour des finalités autres que celles pour lesquelles il a été installé.

Le traitement de données à caractère personnel des salariés qui découlerait de l'usage d'un système de vidéosurveillance à des fins de contrôle des horaires n'apparaît pas nécessaire alors qu'il existe des moyens moins attentatoires à la vie privée des salariés que l'employeur peut mettre en œuvre pour contrôler leurs horaires de travail et leur temps de présence.

En effet, un contrôle des heures de travail par badges via un système de pointeuse est plus efficace et plus protecteur de la vie privée des salariés.

Pour en savoir plus : Lignes directrices « géolocalisation des véhicules » publiées sur le site de la CNPD

RESPECTEZ LES DROITS INDIVIDUELS

Complément : contexte professionnel

Droit d'accès et litiges employé/employeur

Afin de permettre l'exercice ou la défense des droits en justice, le RGPD prévoit des exceptions dans l'exercice des différents droits attribués par le texte. Dans ce cadre strict d'exercice ou de défense des droits en justice, il est permis de traiter des données sensibles ou encore de ne pas répondre favorablement à une demande d'exercice de droit à l'effacement ou de droit d'opposition à un traitement.

Cependant, en ce qui concerne le droit d'accès, l'employeur doit répondre favorablement à la demande de droit d'accès d'un salarié avec lequel il est en conflit (ex: licenciement), même si ces informations pourront être utilisées contre lui; sous peine de violer le RGPD. L'employeur ne doit pas demander au salarié de motiver sa demande. L'employeur doit néanmoins vérifier que cette demande de droit d'accès n'affecte pas de droit des tiers ou le secret des affaires. Le droit d'accès n'est pas un droit absolu (voir *infra*).

Pour en savoir plus : Lignes directrices du CEPD sur le droit d'accès

Droit d'accès et droit des tiers

L'article 15 du RGPD n'opère pas de distinction des données à caractère personnel selon leur origine, en l'occurrence selon que les données ont déjà été fournies dans le passé au responsable du traitement par la personne concernée elle-même ou non (par exemple au moment de la signature d'un contrat de travail). L'ancien employeur doit dès lors fournir ces documents à l'ancien salarié.

En ce qui concerne les échanges de courriels, il est suggéré de demander à la personne concernée de préciser quels sont les courriels visés par sa demande (par exemple, selon la date d'envoi ou de réception, ou selon le destinataire ou l'expéditeur du courriel). La CNPD recommande ensuite d'être particulièrement attentif à éviter la communication de courriels portant atteinte aux droits et libertés d'autrui.

Pour ce faire, le responsable du traitement devrait distinguer les courriels par exemple selon leur nature : les courriels marqués comme « privés » ou « personnels » (dans la mesure où l'ancien employeur en aurait encore possession), ceux concernant exclusivement la relation entre la personne concernée et son employeur (en particulier aux fins de la gestion des ressources humaines), et enfin ceux envoyés ou reçus par la personne concernée en sa qualité de salarié, c'est-à-dire dans le cadre de son activité professionnelle et donc fait au nom et pour le compte de l'employeur. Si cette dernière catégorie de courriel est susceptible de porter atteinte aux droits et libertés d'autrui, en l'occurrence de l'employeur, la communication des courriels privés ou concernant les ressources humaines semble moins problématique en termes d'atteinte potentielle aux droits et libertés d'autrui.

En ce qui concerne des documents internes dans lesquels n'apparaissent que le nom et prénom de l'ancien salarié, il convient de rappeler que ce n'est pas parce que son nom et son prénom figurent dans de tels documents, que cela signifie automatiquement que toutes les informations contenues dans lesdits documents sont à considérer comme des données à caractère personnel concernant l'ancien salarié.

Pour en savoir plus : Fiche pratique et vidéoclip de la CNPD sur le droit d'accès.

Droit d'effacement et contentieux employé/employeur

Le droit à l'effacement existe mais n'est pas un droit absolu.

En effet, aux termes de l'article 17 paragraphe (3) du RGPD, celui-ci ne s'applique pas dans la mesure où ce traitement est nécessaire: a) à l'exercice du droit à la liberté d'expression et d'information; b) pour respecter une obligation légale qui requiert le traitement prévu par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3; d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou e) à la constatation, à l'exercice ou à la défense de droits en justice. Par ailleurs, il convient d'être attentif aux droits des autres personnes qui pourraient être concernées en cas de demande d'effacement.