

Droits des personnes concernées sur leurs données personnelles

La Loi n° 1.565 du 3 décembre 2024 relative à la protection des données liste dans son Chapitre 3 les droits dont dispose chaque personne concernée lors du traitement de ses données à caractère personnel.

Outre le droit à l'information qui impose au responsable du traitement de prendre les mesures appropriées pour fournir toute information à la personne concernée et faciliter l'exercice de ses droits, [Pour plus d'informations, voir la fiche pratique **Information des personnes concernées**], la personne concernée bénéficie de 7 autres droits lui permettant de garder la maîtrise des données la concernant, à savoir :

- le droit d'accès à ses données ;
- le droit de rectification de ses données ;
- le droit à l'effacement de ses données ;
- le droit d'opposition au traitement de ses données ;
- le droit à la limitation du traitement ;
- le droit à la portabilité ;
- le droit de ne pas faire l'objet d'une décision individuelle automatisée.



Le droit d'accès à ses données

L'article 12 de la Loi n° 1.565 du 3 décembre 2024 octroie à toute personne **justifiant de son identité** le droit d'obtenir du responsable du traitement **confirmation que ses données ont été traitées ou le sont encore** et, dans l'affirmative, **leur communication sous une forme lisible et compréhensible**. Le responsable de traitement doit fournir une copie des données traitées.

Exemples :

- une personne peut s'adresser à son employeur pour accéder aux informations la concernant détenues par le Service des Ressources Humaines
- une personne peut s'adresser à une administration pour savoir lesquelles de ses données personnelles sont collectées et à quelles fins

C'est ce qu'on appelle le **droit d'accès**.

La personne concernée a ainsi le droit, « *sous réserve de dispositions législatives spécifiques* », d'obtenir confirmation que ses données sont traitées ainsi que les informations suivantes :

- les **finalités** du traitement, les **catégories de données** et les **destinataires** des informations ;
- la **durée de conservation** des données, ou lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée ;
- en cas de **décision individuelle automatisée**, y compris le **profilage**, le **raisonnement** qui sous-tend le traitement ainsi que **l'importance et les conséquences** prévues pour la personne concernée ;
- la **sources des données** personnelles en cas de collecte indirecte ;
- le droit de demander la **rectification** ou **l'effacement** des données, **une limitation** du traitement ou le droit de **s'opposer** à ce traitement ;
- l'existence d'un **transfert des** informations vers un **pays, un territoire ou une organisation internationale et les garanties appropriées mises en place** ;
- le droit d'introduire une **réclamation auprès de l'APDP**.

Le responsable du traitement doit répondre à une demande de droit d'accès dans le délai **d'un mois suivant la réception de la demande**.

Les informations devront être communiquées dans un **format lisible et compréhensible**, à savoir sous une forme **écrite, non codée et conforme** au contenu du traitement. Le canal de transmission doit être **sécurisé selon la nature et la sensibilité des données** personnelles transmises.



Le responsable du traitement peut exiger le paiement de **frais raisonnables** basés sur les **coûts administratifs pour toute copie supplémentaire demandée** par la personne concernée

Ce droit d'accès est toutefois limité par le **respect du droit des tiers**. Une personne ne peut ainsi avoir **accès qu'aux seules données la concernant**.

Exemple : la personne concernée ne peut demander à obtenir les informations détenues sur un collègue de travail



En cas de **risque de dissimulation ou de disparition des données personnelles**, le président du Tribunal de première instance ou le magistrat délégué par lui statuant en la forme des **référés**, peut ordonner **toutes mesures** de nature à éviter cette dissimulation ou disparition.

Enfin, il est important de noter que le droit d'accès s'exerce généralement **directement** auprès du responsable du traitement mais il peut arriver que ce droit s'exerce **indirectement**. En effet, pour les traitements mis en œuvre **à des fins de prévention et de détection de infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions**, la personne concernée **doit saisir l'APDP** d'une demande de vérification pour savoir si ses données font l'objet d'un traitement.

Le droit d'accès s'exerce également auprès de l'APDP pour les informations personnelles traités en matière de **lutte contre le blanchiment de capitaux**, par les entités assujetties à ces obligations spécifiques.



Le droit de rectification

En vertu de l'article 13 de la Loi n° 1.565 du 3 décembre 2024, la personne concernée « a le droit d'obtenir du responsable du traitement, la rectification, dans les meilleurs délais, de ses données personnelles si celles-ci se révèlent **inexactes** ou **incomplètes** ».

Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire ».

Ce droit de rectification permet ainsi que des données détenues par un responsable du traitement qui se révéleraient **inexactes** ou **incomplètes** soient **rectifiées**, **complétées** ou encore **actualisées**.

Exemples :

- un parent demande à l'école de ses enfants de procéder à la mise à jour de ses coordonnées pour prendre en compte le changement de son numéro de téléphone
- un salarié contacte le Service des Ressources humaines de son entreprise pour obtenir la rectification de son nom de famille qui a été saisi avec une faute d'orthographe



Le responsable du traitement doit notifier à **chaque destinataire** auquel les données personnelles ont été communiquées **toute rectification**, à moins qu'une telle communication se révèle **impossible** ou **exige des efforts disproportionnés**.

Le droit à l'effacement

L'article 14 de la Loi n° 1.565 du 3 décembre 2024 permet à la personne concernée d'obtenir du responsable du traitement, **dans des cas précisément définis**, que ses données soient **effacées**, que celles-ci soient **publiques** ou **non**.



L'exercice de ce droit est **limité aux cas suivants** :

- lorsque la **personne concernée retire son consentement** et qu'il n'existe pas d'autre fondement juridique au traitement (comme par exemple l'intérêt légitime du responsable du traitement) ;
- lorsque la **personne concernée s'oppose au traitement** de ses données, pour des raisons tenant à sa situation particulière à un traitement justifié par l'existence d'un motif d'intérêt public ou la réalisation d'un intérêt légitime, **et qu'il n'existe pas de motif légitime impérieux pour le traitement**, ou qu'elle s'oppose au traitement de ses données à des fins de prospection commerciale ;
- lorsque les **données ne sont plus nécessaires au regard des finalités** pour lesquelles elles ont été collectées ou traitées ;
- lorsque les données ont fait l'objet d'un **traitement illicite** ;
- lorsque les **données ont été collectées dans le cadre d'une offre directe de service de la société de l'information** ;

Qu'entend par offre de service de la société de l'information ?

L'article 2 de la Loi n° 1.565 du 3 décembre 2024 définit un service de la société de l'information comme « *tout service, à titre onéreux ou non, rendu à distance et sans que les parties soient simultanément présentes, par voie électronique et à la demande individuelle d'un destinataire de services.* »

Exemples :

- commande de vêtements sur un site marchand
- abonnement en ligne à une revue électronique

- pour **respecter une obligation légale**.

L'effacement des données doit être réalisé par le responsable du traitement, dans les **meilleurs délais**.

Si les données ont été collectées dans le cadre de **l'offre de services**, que la **personne en fait la demande** et qu'elle était **mineure au moment de la collecte**, le responsable du traitement devra effacer les données dans les **meilleurs délais**. Si le responsable du traitement a transmis ces données à un tiers, lui-même responsable du traitement, il devra prendre des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre pour informer le tiers qui traite lesdites données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou reproduction de celles-ci.



Si le responsable du traitement n'a pas effacé les données dans un délai d'un mois, à compter de la demande, ou s'il n'a pas répondu dans ce délai, la personne concernée pourra **saisir l'APDP**.

En revanche, ce **droit à l'effacement ne s'applique pas** lorsque le traitement est nécessaire :

- pour respecter **une obligation légale** qui requiert le traitement de ces données ;
- pour exercer une **mission d'intérêt général par une personne morale de droit privé qui en est investie ou concessionnaire d'un service public** ;
- pour exercer une **mission relevant de l'exercice de l'autorité publique** dont est investi le responsable du traitement ;
- à des **fins archivistiques** dans l'intérêt public, à des **fins de recherche scientifique ou historique** ou à des **fins statistiques**, dans la mesure où l'exercice de ce droit est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ;
- pour la **constatation, l'exercice ou la défense de droits en justice** ;
- pour l'exercice du **droit à la liberté d'expression publique et d'information**.

Exemple : Un traitement mis en œuvre par le Centre Hospitalier Princesse Grace dans le domaine de la santé publique

Enfin, un **responsable du traitement qui a rendu les données personnelles publiques** doit informer, par des **mesures raisonnables, compte tenu des technologies disponibles et des coûts de mise en œuvre**, les autres responsables du traitement qui traitent ces données afin qu'ils effacent tout lien vers ces données ainsi que toute copie ou reproduction.



Le responsable du traitement doit notifier à **chaque destinataire** auquel les données personnelles ont été communiquées **tout effacement**, à moins qu'une telle communication se révèle **impossible** ou **exige des efforts disproportionnés**.

Le droit à la limitation du traitement

Ce nouveau droit introduit par l'article 15 de la Loi n° 1.565 du 3 décembre 2024 permet à la personne concernée d'obtenir, du responsable de traitement, la limitation du traitement, à savoir le « **gel pendant une certaine durée** » du traitement de ses données, sauf pour leur conservation.



Ce droit s'applique dans **4 cas** :

- la personne concernée **conteste l'exactitude des données** (leur traitement sera alors limité le temps de la vérification de leur exactitude) ;
- le **traitement n'est pas licite** mais la **personne concernée ne souhaite pas l'effacement des données** ;
- le traitement **ne se justifie plus par sa finalité** mais la personne veut faire constater, exercer ou défendre **ses droits en justice** ;
- le traitement est **justifié par des motifs légitimes** poursuivis par le responsable du traitement et **la personne concernée en conteste la légitimité**. Le responsable du traitement va alors « *geler* » le traitement le temps de savoir si ses motifs légitimes prévalent sur ceux de la personne concernée.

Exemple : une personne concernée pourra demander que des images de vidéosurveillance qui sont normalement supprimées par le responsable du traitement au bout de 30 jours, soient conservées au-delà de ce délai dans le cadre d'une procédure judiciaire

Si les données personnelles ayant fait l'objet d'une limitation **peuvent être conservées**, elles **ne peuvent en principe pas être traitées à d'autres fins**.

Le responsable du traitement doit **informer sans délai** la personne concernée de la limitation du traitement de ses données.



Le responsable du traitement doit également notifier à **chaque destinataire** auquel les données personnelles ont été communiquées **toute limitation**, à moins qu'une telle communication se révèle **impossible** ou **exige des efforts disproportionnés**.

Le deuxième alinéa de l'article 15 dispose néanmoins que les données personnelles concernées par l'exercice de ce droit **peuvent être traitées**, dans les 3 situations suivantes :

- avec le **consentement** de la personne concernée ;
- pour la **constatation, l'exercice ou la défense de droits en justice** pour la **protection des droits d'une autre personne physique ou morale** ; ou
- pour des **motifs importants d'intérêt public**.

Comment le responsable du traitement peut-il limiter le traitement des données ?

Différentes méthodes sont possibles, telles que :

- le déplacement des données concernées vers un autre système de traitement ;
- le retrait des données publiées sur un site Internet ;
- le blocage de l'accès des utilisateurs à ces données.

La limitation peut également être **techniquement assurée**, en identifiant les données comme appartenant à un traitement faisant l'objet d'une limitation ce qui rendra impossible leur modification ou traitement.

L'exercice du droit à la limitation n'est pas applicable aux traitements :

- **mis en œuvre 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
- **mis en œuvre par les autorités administratives et judiciaires**, agissant dans le cadre de leurs prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes ;
- qui intéressent la **sécurité nationale**.

Le droit d'opposition

La personne concernée dispose d'un droit d'opposition au traitement de ses données à caractère personnel prévu à l'article 17 de la Loi n° 1.565 du 3 décembre 2024

Ce droit s'exerce différemment selon les finalités du traitement.

Le droit d'opposition pour des raisons tenant à la situation particulière de la personne concernée

Le premier alinéa de l'article 17 de la Loi précise que la personne a le droit de s'opposer au traitement de ses données personnelles pour des raisons tenant à **sa situation particulière** dès lors que ce traitement est fondé sur :

- l'existence d'un **motif d'intérêt public** lorsque les traitements sont mis en œuvre par une personne morale de droit public ou par une personne morale de droit privé investie d'une mission d'intérêt général ou concessionnaire d'un service public ;
- la **réalisation d'un intérêt légitime** poursuivi par le responsable du traitement.



Le responsable du traitement doit informer **clairement** la personne concernée de son droit d'opposition **au plus tard au moment de la première communication** de manière **séparée de toute autre information**.

Le responsable du traitement ne pourra alors plus traiter les données personnelles, à moins de **démontrer qu'il existe des motifs légitimes et impérieux** pour le traitement qui **prévalent sur les intérêts et les droits et libertés de la personne concernée**, ou pour la constatation, l'exercice ou la défense de droits en justice.



La **charge de la preuve** incombe au **responsable du traitement** qui doit prouver, **au cas par cas**, l'existence de **motifs impérieux** justifiant la poursuite du traitement.

Le droit d'opposition à l'utilisation des données à des fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection

La personne concernée a le droit de s'opposer **à tout moment** au traitement de ses données **sans avoir à justifier** l'exercice de ce droit d'opposition auprès du responsable du traitement qui sera **tenu d'y faire droit**.

Les données ne seront alors plus traitées à ces fins.

Dans le cadre de l'utilisation de services de la société de l'information

La personne concernée peut exercer son droit d'opposition à l'aide de **procédés automatisés** utilisant des spécifications techniques.

Le responsable du traitement qui propose des services de la société de l'information doit donc mettre en place des **procédures et des modalités techniques adéquates** pour garantir l'effectivité du droit d'opposition.

Exemple : désactiver le suivi de la navigation sur internet

Le droit d'opposition au traitement à des fins de recherche scientifique ou historique ou à des fins statistiques

La personne concernée a le droit de **s'opposer** au traitement, à des fins de **recherche scientifique, historique ou statistique**, de ses données **pour des raisons tenant à sa situation particulière**.

Cependant, il n'y a **pas de droit d'opposition si le traitement est nécessaire à l'exécution d'une mission d'intérêt général** par une personne morale de droit privé ou concessionnaire d'un service public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

L'exercice du droit d'opposition n'est pas applicable aux traitements :

- **mis en œuvre 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
- **mis en œuvre par les autorités administratives et judiciaires**, agissant dans le cadre de leurs prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes ;
- qui intéressent la **sécurité nationale**.



Le droit à la portabilité

L'art 18 de la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles dispose que :

« La personne concernée a le droit de recevoir ses données personnelles qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et a le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle ».

Ce nouveau droit permet ainsi à la personne concernée :

- **d'obtenir** du responsable du traitement les données personnelles qu'elle lui a fournies et de les réutiliser, mais aussi ,
- de **les confier à un autre responsable du traitement** dans le même secteur d'activité ou dans un autre.

Le but est de **renforcer le contrôle que les personnes concernées exercent sur leurs propres données** en leur permettant de sauvegarder leurs données en vue d'un **usage personnel ultérieur** ou de les **transmettre facilement d'un environnement numérique à un autre**, que celui-ci soit le leur, celui d'un nouveau responsable du traitement ou bien encore celui d'un tiers qu'elles désignent.

Quelles sont les conditions d'application du droit à la portabilité ?

Celles-ci sont au nombre de deux :

- les données traitées doivent être justifiées par le **consentement de la personne concernée** ou être **nécessaires** à l'exécution d'un **contrat**.

Le droit à la portabilité des données ne s'applique donc pas au traitement nécessaire à l'exécution d'une mission d'intérêt général par une personne morale de droit privé qui en est investie ou concessionnaire d'un service public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Exemples :

- l'historique des achats d'un consommateur sur un site Internet peut faire l'objet du droit à la portabilité car il a été constitué sur la base de l'exécution d'un contrat auquel ledit consommateur est partie
- les données collectées par un établissement financier dans le cadre de son devoir de vigilance, notamment en matière de lutte contre le blanchiment d'argent, ne relèvent pas en revanche du champ d'application de la portabilité car leur traitement est justifié par le besoin de respecter une obligation légale à laquelle est soumis le responsable

- le traitement doit être effectué à l'aide de **procédés automatisés**.

La plupart des dossiers papiers ne sont donc pas couverts par ce droit, sauf à avoir été automatisés.

L'exercice de ce droit ne doit **pas porter atteinte aux droits et libertés des tiers**.

Conformément aux Lignes directrices relatives au droit à la portabilité des données adoptées le 13 décembre 2016 par le Groupe de travail « Article 29 » (GT art. 29)¹, un « nouveau » responsable du traitement destinataire « *ne peut pas utiliser les données de tiers qui lui sont transmises à des fins qui lui sont propres, par exemple pour proposer des produits et services de marketing à ces autres tierces personnes concernées* ».



Lesdites Lignes directrices recommandent de mettre en œuvre « *des outils permettant aux personnes concernées de choisir les données qu'elles souhaitent recevoir et transmettre* ».

Quelles sont les données concernées par le droit à la portabilité ?

Les données pouvant être transmises dans le cadre de l'exercice du droit à la portabilité des données sont :

- **les données relatives à la personne concernée.**

Seules les données à caractère personnel peuvent faire l'objet d'une demande de droit à la portabilité. Dès lors, conformément aux Lignes directrices du GT art.29 précitées, les données anonymisées sont exclues du droit à la portabilité puisqu'elles ne permettent plus l'identification de la personne concernée.



Les **données pseudonymisées** qui peuvent clairement être liées à la personne concernée, notamment lorsque celle-ci fournit l'identifiant correspondant, relèvent du champ d'application du droit à la portabilité.

- **les données fournies par la personne concernée :**
 - soit **activement et sciemment** ;
 - soit **découlant de l'observation** de l'activité de cette dernière.

Exemples :

- l'historique d'utilisation d'un site internet
- les données d'objets connectés
- les activités de recherche sur internet
- les données de localisation d'une personne

¹ Groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018 (avant l'entrée en vigueur du Règlement Général sur la Protection des Données - RGPD).



Sont en revanche exclues du champ d'application, les **données déduites et les données dérivées**, à savoir les données créées par le responsable du traitement sur la base des données fournies par la personne.

Exemple : une appréciation relative à la santé d'un utilisateur

Sous quel format doivent être communiquées les données ?

La Loi prévoit que les données doivent être fournies dans un format :

- structuré ;
- couramment utilisé ;
- lisible par machine.

Le format le plus approprié différera d'un secteur à l'autre.

La personne concernée a par ailleurs le droit d'obtenir que ses données personnelles soient transmises **directement d'un responsable du traitement à un autre** lorsque cela est **techniquement possible** : communication authentifiée avec un niveau de chiffrement nécessaire.

Le droit de ne pas faire l'objet d'une décision individuelle automatisée

En vertu de l'article 19 de la Loi, « La personne concernée a le droit de ne pas faire l'objet d'une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé, y compris le profilage ».

Qu'est-ce que le profilage ?

L'article 2 de la Loi n° 1.565 du 3 décembre 2024 définit le profilage comme :

« toute forme de traitement automatisé de données à caractère personnel consistant à utiliser celles-ci pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».



Une décision individuelle automatisée peut être fondée ou non sur le profilage, mais tout profilage n'implique pas nécessairement une prise de décision individuelle automatisée.

Il ressort de cette définition qu'une personne concernée ne peut pas faire l'objet d'une décision qui repose **exclusivement** sur un traitement automatisé, **sans aucune intervention humaine** lorsque la décision **produit des effets juridiques** à l'égard de la personne concernée ou **l'affecter de manière significative**.

Ce droit à ainsi vocation à protéger la personne concernée face à des décisions impactant ses droits et libertés en **influençant son environnement, son comportement et son choix** ou **aboutissant à une discrimination**.

Exemple : un établissement financier qui décide ou non d'accorder un prêt sur la seule base d'un algorithme qui évalue la solvabilité du demandeur

Des exceptions à cette interdiction sont toutefois admises dans 4 cas bien précis.

- lorsque la décision est prise **dans le cadre de la conclusion ou de l'exécution d'un contrat** entre la personne concernée et un responsable de traitement, **à condition** que la demande de conclusion ou d'exécution du contrat, **introduite par la personne concernée ait été satisfaite**. Le responsable du traitement doit mettre en œuvre des **mesures appropriées** pour la **sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée**, au moins du droit de la personne concernée d'obtenir **une intervention humaine** de la part du responsable du traitement, **d'exprimer son point de vue et de contester la décision**.
- lorsque la décision est autorisée par des **dispositions législatives ou réglementaires** qui précisent les **mesures garantissant la sauvegarde des droits et libertés** et de **l'intérêt légitime de la personne concernée**.
- lorsque la décision est fondée sur le **consentement explicite de la personne concernée**. Le responsable du traitement doit mettre en œuvre des **mesures appropriées** pour la **sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée**, au moins du droit de la personne concernée d'obtenir **une intervention humaine** de la part du responsable du traitement, **d'exprimer son point de vue et de contester la décision**.
- lorsqu'en présence de **données sensibles**, la décision est **fondée sur le consentement explicite** de la personne concernée **ou justifiée par des motifs d'intérêt public**. Le responsable du traitement doit mettre en œuvre des **mesures appropriées** pour la **sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée**, au moins du droit de la personne concernée d'obtenir **une intervention humaine** de la part du responsable du traitement, **d'exprimer son point de vue et de contester la décision**.

Cas particulier des personnes décédées

L'article 20 de la Loi n° 1.565 du 3 décembre 2024, prévoit que sauf dispositions législatives et réglementaires contraires, les personnes suivantes :

- l'**ascendant** ,
- le **descendant jusqu'au second degré** ,
- le **conjoint survivant** d'une personne décédée ,
- le **cohabitant** ou le **partenaire** au sens de la Loi n°1.481 du 17 décembre 2019,

peuvent, **si elles justifient d'un intérêt**, exercer les droits suivants en ce qui concerne les informations relatives aux personnes décédées :

- le droit **d'accès** ;
- le droit de **rectification** ;
- le droit d'**effacement** ;
- le droit à la **limitation du traitement** ;
- le droit d'**opposition** ;
- le droit à la **portabilité**.

Outre la justification de leur identité, ces personnes devront apporter la **preuve de leur lien avec la personne décédée par tout moyen**.

Quelle est la sanction encourue en cas de manquement aux obligations relatives aux droits des personnes concernées ?

L'article 54 de la Loi n° 1.565 du 3 décembre 2024 prévoit que le manquement aux obligations relatives aux droits des personnes concernées est puni d'une amende administrative ne pouvant excéder **10.000.000 euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu**.