Conseil de
l'Union européenne

Bruxelles, le 11 juin 2015
(OR. en)

9565/15

Dossier interinstitutionnel:
2012/0011 (COD)

DATAPROTECT 97
JAI 420
MI 369
DIGIT 49
DAPIX 94
FREMP 133
COMIX 259
CODEC 823

NOTE

Origine:	la présidence
Destinataire:	Conseil
Nº doc. préc.:	9398
Objet:	Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données) - Préparation d'une orientation générale

Introduction

Le 25 janvier 2012, la Commission a adopté sa proposition de règlement général sur la protection des données (doc. 5853/15). Le nouveau règlement est destiné à remplacer la directive 95/46/CE. Son objectif est double: renforcer les droits des personnes physiques en matière de protection des données et améliorer les débouchés commerciaux en facilitant le libre flux des données à caractère personnel dans le marché unique numérique.

Parallèlement à la proposition de règlement général sur la protection des données, la Commission a adopté une communication fixant ses objectifs (doc. 5852/12) et une directive relative au traitement de données à des fins répressives (doc. 5833/12). La nouvelle directive est destinée à remplacer la décision-cadre de 2008 sur la protection des données.

Le 12 mars 2014, le Parlement européen a adopté ses positions en première lecture concernant la proposition de règlement sur la protection des données et la proposition de directive relative à la protection des données.

Texte de compromis

Plusieurs orientations générales partielles ont contribué à ce que les avis exprimés au sein du Conseil convergent sur l'ensemble du règlement général sur la protection des données. On trouvera en annexe le texte du règlement que la présidence présente pour approbation sous forme d'orientation générale. Toutes les modifications apportées à la proposition initiale de la Commission apparaissent en caractères soulignés; les suppressions sont indiquées par (…). Le texte existant qui a été déplacé est en *italique*. Les commentaires des délégations sur le texte du règlement - qui ne contenait pas encore les nouvelles suggestions de la présidence pour les considérants 118 et 134 - sont reflétées dans les résultats des travaux menés par le Comité des représentants permanents lors de sa réunion du 9 juin 2015 (doc. 9788/15).

Compte tenu de la réunion tenue par le Comité des représentants permanents le 9 juin 2015, la présidence a apporté deux changements.

Droit à réparation et responsabilité - Article 77 et considérant 118

La présidence suggère de modifier le considérant 118 afin de préciser que l'objectif général de l'article 77 et du considérant 118 est de faire en sorte que la personne concernée soit effectivement et intégralement indemnisée pour le dommage subi. Compte tenu des différences entre les systèmes juridiques des États membres en matière de responsabilité, la personne concernée peut recevoir une indemnisation du responsable du traitement ou du sous-traitant qui est tenu responsable du dommage dans son ensemble ou, dans les États membres dont les systèmes juridiques permettent des actions conjointes, cette indemnisation peut être imputée à plusieurs responsables du traitement ou sous-traitants.

Application du règlement - considérant 134

En de garantir une sécurité juridique suffisante aux responsables du traitement et aux sous-traitants dont le traitement actuel des données à caractère personnel est conforme à la directive 95/46/CE, la présidence suggère de clarifier le champ d'application du règlement dans le considérant 134.

Conclusion

En vue d'octroyer à la présidence un mandat lui permettant d'engager des négociations avec les représentants du Parlement européen, le Conseil est invité à approuver le texte du règlement général sur la protection des données tel qu'il figure en annexe sous forme d'orientation générale.

ANNEXE

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

Protection des données à caractère personnel: traitement et libre circulation des données (règlement général sur la protection des données)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16, paragraphe 2 (…),

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen,

après consultation du contrôleur européen de la protection des données,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe 1, du traité disposent que toute personne a droit à la protection des données à caractère personnel la concernant.

(2) (…) Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes, respecter leurs libertés et leurs droits fondamentaux, notamment le droit à la protection des données à caractère personnel. Le traitement des données devrait contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes.

(3) La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données vise à harmoniser la protection des libertés et des droits fondamentaux des personnes physiques en ce qui concerne les activités de traitement de données et à garantir la libre circulation des données à caractère personnel entre les États membres.

(3 *bis*) (…) Le droit à la protection des données à caractère personnel n'apparaît pas comme une prérogative absolue; il doit être pris en considération par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les principes reconnus par la Charte des droits fondamentaux de l'Union européenne, consacrés par les traités, et notamment le droit au respect de la vie privée et familiale, du domicile et des communications, le droit à la protection des données à caractère personnel, le droit à la liberté de pensée, de conscience et de religion, le droit à la liberté d'expression et d'information, le droit à la liberté d'entreprise, le droit à un recours effectif et à un procès équitable, ainsi que le respect de la diversité culturelle, religieuse et linguistique.

(4) L'intégration économique et sociale résultant du fonctionnement du marché intérieur a conduit à une augmentation substantielle des flux transfrontières. Les échanges de données entre (…) acteurs publics et privés, y compris les personnes physiques et les entreprises, se sont intensifiés dans l'ensemble de l'Union. Le droit de l'Union appelle les autorités nationales des États membres à coopérer et à échanger des données à caractère personnel, afin d'être en mesure de remplir leurs missions ou d'accomplir des tâches pour le compte d'une autorité d'un autre État membre.

(5) L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. La collecte et le partage de données ont connu une augmentation spectaculaire. Les nouvelles technologies permettent tant aux entreprises privées qu'aux pouvoirs publics d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus de personnes physiques rendent des informations les concernant accessibles à tout un chacun, où qu'il se trouve dans le monde. Les nouvelles technologies ont ainsi transformé l'économie et les rapports sociaux, et elles devraient faciliter davantage la libre circulation des données au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel.

(6) Cette évolution requiert (...) un cadre de protection des données plus solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, compte tenu de l'importance de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur. Les personnes physiques devraient maîtriser l'utilisation qui est faite des données à caractère personnel les concernant, et la sécurité tant juridique que pratique devrait être renforcée pour les particuliers, les opérateurs économiques et les autorités publiques.

(6 *bis*) Lorsque le présent règlement dispose que la législation des États membres apporte des précisions ou des limitations aux règles qu'il prévoit, les États membres peuvent intégrer des éléments du présent règlement dans leur propre droit national dans la mesure nécessaire pour garantir la cohérence et pour rendre les dispositions nationales compréhensibles pour les personnes auxquelles elles s'appliquent.

(7) Si elle demeure satisfaisante en ce qui concerne ses objectifs et ses principes, la directive 95/46/CE n'a pas permis d'éviter une fragmentation de la mise en œuvre de la protection des données à caractère personnel dans l'Union, une insécurité juridique et le sentiment, largement répandu dans le public, que des risques importants subsistent, notamment dans l'environnement en ligne. Si le niveau de protection des droits et libertés des personnes physiques - notamment du droit à la protection des données à caractère personnel - accordé dans les États membres à l'égard du traitement des données à caractère personnel n'est pas identique, cela risque d'entraver la libre circulation de ces données dans l'ensemble de l'Union. Ces différences peuvent dès lors constituer un obstacle à l'exercice des activités économiques au niveau de l'Union, fausser la concurrence et empêcher les autorités de s'acquitter des obligations qui leur incombent en vertu du droit de l'Union. Ces écarts de niveau de protection résultent de l'existence de divergences dans la transposition et l'application de la directive 95/46/CE.

(8) Afin d'assurer la cohérence et un degré élevé de protection des personnes, et de lever les obstacles à la circulation des données à caractère personnel au sein de l'Union, le niveau de protection des droits et des libertés des personnes à l'égard du traitement de ces données devrait être équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union. En ce qui concerne les traitements de données à caractère personnel nécessaires au respect d'une obligation légale, à l'exécution d'une tâche réalisée dans l'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, il y a lieu d'autoriser les États membres à maintenir ou à introduire des dispositions nationales destinées à mieux préciser l'application des règles prévues dans le présent règlement. Parallèlement à la législation générale et horizontale relative à la protection des données mettant en œuvre la directive 95/46/CE, les États membres disposent de plusieurs lois sectorielles spécifiques dans des domaines qui requièrent des dispositions plus précises. Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles. Dans les limites de cette marge de manœuvre, les législations sectorielles spécifiques que les États membres ont adoptées en vue de mettre en œuvre la directive 95/46/CE devraient pouvoir être maintenues.

(9) Une protection effective des données à caractère personnel dans toute l'Union exige non seulement de renforcer et de préciser les droits des personnes concernées, ainsi que les obligations de ceux qui effectuent ou déterminent le traitement des données à caractère personnel, mais aussi de conférer, dans les États membres, des pouvoirs équivalents de surveillance et de contrôle de l'application des règles relatives à la protection des données à caractère personnel, et de prévoir des sanctions équivalentes pour les contrevenants.

(10) L'article 16, paragraphe 2, du traité donne mandat au Parlement européen et au Conseil pour fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ainsi que les règles relatives à la libre circulation de ces données.

(11) Afin d'obtenir un niveau uniforme de protection des personnes physiques dans toute l'Union, et d'éviter que des divergences n'entravent la libre circulation des données au sein du marché intérieur, un règlement est nécessaire pour garantir la sécurité juridique et la transparence aux opérateurs économiques, notamment les micro, petites et moyennes entreprises, pour assurer aux personnes de tous les États membres un même niveau de droits opposables, et des obligations et responsabilités égales pour les responsables du traitement des données et les sous-traitants (...), de même que pour assurer une surveillance cohérente du traitement des données à caractère personnel, des sanctions équivalentes dans tous les États membres et une coopération efficace entre les autorités de contrôle des différents États membres. Pour que le marché intérieur fonctionne correctement, il faut que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. (...)

Le présent règlement comporte un certain nombre de dérogations visant à tenir compte de la situation particulière des micro, petites et moyennes entreprises. Les institutions et organes de l'Union, les États membres et leurs autorités de contrôle sont, en outre, encouragés à prendre en considération les besoins spécifiques des micro, petites et moyennes entreprises dans le cadre de l'application du présent règlement. Pour définir la notion de micro, petites et moyennes entreprises, il convient de s'inspirer de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises.

(12) La protection conférée par le présent règlement concerne les personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, dans le cadre du traitement des données à caractère personnel. En ce qui concerne le traitement de données relatives à des personnes morales, et en particulier des entreprises dotées de la personnalité juridique, notamment le nom, la forme juridique et les coordonnées de la personne morale, la protection conférée par le présent règlement ne devrait pas pouvoir être invoquée par ces personnes. (...).

(13) La protection des personnes physiques devrait être neutre sur le plan technologique et ne pas dépendre des techniques utilisées, sous peine de créer de graves risques de contournement. Elle devrait s'appliquer aux traitements de données à caractère personnel automatisés ainsi qu'aux traitements manuels si les données sont contenues ou destinées à être contenues dans un fichier. Les dossiers ou ensembles de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés, ne devraient pas relever du champ d'application du présent règlement.

(14) Le présent règlement ne traite pas des questions de protection des libertés et droits fondamentaux ou de libre circulation des données relatives à des activités n'entrant pas dans le champ d'application du droit de l'Union, telles que les activités relatives à la sécurité nationale (…), ni du traitement des données à caractère personnel par les États membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union.

(14 *bis*) Le règlement (CE) nº 45/2001 s'applique au traitement des données à caractère personnel par les institutions, organes, organismes et agences de l'Union. Le règlement (CE) nº 45/2001 et les autres instruments juridiques de l'Union applicables au traitement des données à caractère personnel devraient être adaptés aux principes et aux règles du présent règlement.

(15) Le présent règlement ne devrait pas s'appliquer aux traitements de données à caractère personnel effectués par une personne physique pour l'exercice d'activités personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles et domestiques incluent l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités personnelles et domestiques. Toutefois, le présent règlement devrait s'appliquer aux (…) responsables du traitement de données ou à leurs sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.

(16) La protection des personnes physiques à l'égard du traitement des données à caractère personnel effectué par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière**,** d'exécution de sanctions pénales ou de protection contre les menaces à l'encontre de la sécurité publique et de prévention de telles menaces, ainsi que la libre circulation de ces données, font l'objet d'un instrument juridique spécifique au niveau de l'Union.

Le présent règlement ne devrait donc pas s'appliquer aux activités de traitement effectuées à ces fins. Toutefois, le traitement de données à ces fins par des autorités publiques devrait être régi par cet instrument juridique plus spécifique au niveau de l'Union (à savoir la directive XX/YYY). Les États membres peuvent confier à des autorités compétentes au sens de la directive XX/YYY d'autres tâches qui ne sont pas nécessairement menées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou de protection contre les menaces à l'encontre de la sécurité publique et de prévention de telles menaces, de manière à ce que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application de la législation de l'Union, relève du champ d'application du présent règlement.

En ce qui concerne le traitement de données à caractère personnel par ces autorités compétentes à des fins relevant du champ d'application du règlement général sur la protection des données, les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du règlement général sur la protection des données. Ces dispositions peuvent déterminer plus précisément les exigences spécifiques au traitement de données à caractère personnel par ces autorités compétentes à ces autres fins, compte tenu de la structure constitutionnelle, organisationnelle et administrative de l'État membre concerné.

Lorsque le traitement de données à caractère personnel par (…) des organismes privés relève du champ d'application du présent règlement, celui-ci devrait prévoir la possibilité pour les États membres, sous certaines conditions, de limiter par la loi certaines obligations et certains droits lorsque cette limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour préserver des intérêts majeurs spécifiques tels que la sécurité publique, ainsi que la prévention et la détection des infractions pénales et les enquêtes et les poursuites en la matière. Cela est important, par exemple, dans le cadre de la lutte contre le blanchiment d'argent ou des activités des laboratoires de police scientifique.

(16 *bis*) *Bien que le présent règlement s'applique également aux activités des juridictions* et autres autorités judiciaires, l'Union ou les États membres pourraient préciser quelles sont les opérations de traitement et les procédures de traitement de données à caractère personnel des juridictions et autres autorités judiciaires. *La compétence des autorités de contrôle ne devrait pas s'étendre au traitement de données à caractère personnel par les juridictions lorsqu'elles agissent dans le cadre de leur fonction juridictionnelle*, afin de préserver l'indépendance du pouvoir judiciaire dans le cadre de ses fonctions juridictionnelles, y compris lorsqu'il prend des décisions. Le contrôle du traitement des données peut être confié à des organes spécifiques du pouvoir judiciaire de l'État membre, qui devraient notamment contrôler le respect des dispositions du présent règlement, sensibiliser le pouvoir judiciaire aux obligations qui lui incombent en vertu du présent règlement et gérer les réclamations formulées à l'égard de ce traitement.

(17) La directive 2000/31/CE ne s'applique pas aux questions relatives aux services de la société de l'information couvertes par le présent règlement. Ladite directive a pour objectif de contribuer au bon fonctionnement du marché intérieur en assurant la libre circulation des services de la société de l'information entre les États membres. Il convient que le présent règlement ne porte pas atteinte à son application. Le présent règlement devrait par conséquent s'appliquer sans préjudice de la directive 2000/31/CE, et notamment de ses articles 12 et 15 relatifs à la responsabilité des prestataires intermédiaires.

(18) (…)

(19) Tout traitement de données à caractère personnel intervenant dans le cadre des activités d'un établissement d'un responsable du traitement ou sous-traitant situé sur le territoire de l'Union devrait être effectué conformément au présent règlement, que le traitement lui-même se déroule à l'intérieur de l'Union ou non. L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

(20) Afin d'éviter qu'une personne physique soit exclue de la protection qui lui est garantie en vertu du présent règlement, le traitement de données à caractère personnel relatives à des personnes concernées résidant dans l'Union par un responsable du traitement qui n'est pas établi dans l'Union devrait être soumis au présent règlement lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non. Afin de déterminer si un tel responsable du traitement offre des biens ou des services à des personnes concernées dans l'Union, il y aurait lieu d'examiner s'il apparaît que le responsable du traitement envisage de faire affaire avec des personnes concernées résidant dans un ou plusieurs États membres de l'Union. Considérant que la seule accessibilité du site Internet du responsable du traitement ou d'un intermédiaire dans l'Union ou d'une adresse électronique et d'autres coordonnées ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffisent pas pour établir cette intention, des facteurs tels que l'utilisation d'une langue ou d'une monnaie généralement utilisées dans un ou plusieurs États membres avec la possibilité de commander des biens et des services dans cette autre langue et/ou la mention de clients ou d'utilisateurs résidant dans l'Union peuvent indiquer que le responsable du traitement envisage d'offrir des biens ou des services à ces personnes concernées dans l'Union.

(21) Le traitement de données à caractère personnel concernant des personnes résidant dans l'Union par un responsable du traitement qui n'est pas établi dans l'Union devrait également être soumis au présent règlement lorsqu'il est lié à l'observation de leur comportement au sein de l'Union européenne. Afin de déterminer si une activité de traitement peut être considérée comme "une observation" du comportement des personnes concernées, il y a lieu d'établir si ces personnes sont suivies sur Internet au moyen de techniques de traitement de données consistant à analyser le profil d'un individu, afin notamment de prendre des décisions le concernant ou d'analyser ou de prévoir ses préférences, son comportement et sa disposition d'esprit.

(22) Lorsque le droit national d'un État membre s'applique en vertu du droit international public, le présent règlement devrait s'appliquer également à un responsable du traitement de données qui n'est pas établi dans l'Union mais, par exemple, dans une mission diplomatique ou un poste consulaire d'un État membre.

(23) Il y a lieu d'appliquer les principes de protection des données à toute information concernant une personne physique identifiée ou identifiable. Il convient de considérer les données pseudonymisées qu'il a été possible d'attribuer à une personne physique en utilisant des informations supplémentaires comme des informations concernant une personne physique identifiable. Pour déterminer si une personne est identifiable, il faut considérer l'ensemble des moyens raisonnablement susceptibles d'être mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier directement ou indirectement ladite personne. Pour établir si des moyens sont raisonnablement susceptibles d'être mis en œuvre afin d'identifier une personne physique, il convient de considérer l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte à la fois des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a donc pas lieu d'appliquer les principes de protection des données aux informations anonymes, à savoir aux informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données rendues anonymes pour que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique par conséquent pas au traitement de ces informations anonymes, y compris à des fins statistiques et de recherche.

(23 *bis bis*) Il n'y a pas lieu d'appliquer les principes de protection des données aux données concernant des personnes décédées. Le droit national d'un État membre peut prévoir des règles relatives au traitement des données à caractère personnel concernant des personnes décédées.

(23 *bis*) La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à respecter leurs obligations en matière de protection des données. L'introduction explicite de la "pseudonymisation" par l'intermédiaire des articles du présent règlement ne vise donc pas à exclure toute autre mesure de protection des données.

(23 *ter*) (…)

(23 *quater*) Afin d'encourager la pseudonymisation dans le cadre du traitement des données à caractère personnel, il convient que les mesures de pseudonymisation, tout en permettant une analyse générale, puissent être prises chez un même responsable du traitement lorsque celui-ci a pris les mesures techniques et organisationnelles nécessaires pour que les dispositions du présent règlement soient mises en œuvre, en tenant compte des traitements respectifs des données et en veillant à ce que les informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée spécifique soient conservées à part. L'expression "responsable du traitement qui traite les données" désigne également les personnes autorisées chez un même responsable du traitement. Dans ce cas, toutefois, le responsable du traitement s'assure que les personnes qui effectuent la pseudonymisation ne sont pas référencées dans les métadonnées.

(24) Lorsqu'elles utilisent des services en ligne, les personnes physiques se voient associer des identifiants en ligne tels que des adresses IP ou des témoins de connexion ("cookies") par les appareils, applications, outils et protocoles utilisés. Ces identifiants peuvent laisser des traces qui, si elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils et à identifier les personnes. Les numéros d'identification, les données de localisation, les identifiants en ligne ou d'autres éléments spécifiques ne devraient pas être (…) considérés, en soi, comme des données à caractère personnel s'ils n'identifient pas ou ne rendent pas identifiable une personne physique.

(25) Le consentement devrait être donné sans ambiguïté, selon toute modalité appropriée permettant une manifestation de volonté libre, spécifique et informée, consistant soit en une déclaration écrite, y compris électronique, ou une déclaration orale, soit, si des circonstances spécifiques le requièrent, en tout autre acte positif univoque de la personne concernée indiquant qu'elle accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. La personne concernée peut, par exemple, donner son consentement en cochant une case lorsqu'elle consulte un site Internet ou par le biais de toute déclaration ou de tout comportement indiquant clairement dans ce contexte qu'elle accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement tacite ou passif. Lorsque cela est techniquement possible et opérant, la personne concernée peut donner son consentement en utilisant les paramètres appropriés d'un navigateur ou d'une autre application. Dans ce cas, il suffit que la personne concernée reçoive les informations nécessaires pour donner son consentement libre, spécifique et informé au moment de commencer à utiliser le service. (…). Le consentement donné devrait valoir pour toutes les activités de traitement ayant la même finalité. Lorsque le traitement a plusieurs finalités, un consentement sans ambiguïté devrait être donné pour l'ensemble des finalités du traitement. Si le consentement de la personne concernée est donné à la suite d'une demande par voie électronique, cette demande doit être claire, concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé.

(25 *bis*) Les données génétiques devraient être définies comme les données à caractère personnel liées aux caractéristiques génétiques d'une personne physique qui sont héréditaires ou ont été acquises et résultant d'une analyse d'un échantillon biologique de la personne en question, notamment par une analyse des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou d'une analyse de tout autre élément permettant d'obtenir des informations équivalentes.

(25 *bis bis*) Souvent, il n'est pas possible de cerner entièrement l'objectif du traitement des données à des fins scientifiques au moment de la collecte des données. Par conséquent, les personnes concernées peuvent donner leur consentement pour ce qui concerne certains domaines de la recherche scientifique, lorsque les normes éthiques reconnues en matière de recherche scientifique sont respectées. Les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet et pour autant que cela n'implique pas d'efforts disproportionnés au regard de l'objectif de protection poursuivi.

(26) Les données à caractère personnel concernant la santé devraient comprendre (…) les données se rapportant à l'état de santé d'une personne concernée qui comportent des informations sur la santé physique ou mentale passée, présente ou future de la personne concernée, y compris des informations relatives à l'enregistrement du patient pour la prestation de services de santé (…), un numéro ou un symbole attribué à un patient, destinés à l'identifier de manière univoque à des fins médicales, (…) des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des données génétiques et des échantillons biologiques, (…) ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostique in vitro.

(27) Le principal établissement d'un responsable du traitement dans l'Union devrait être le lieu de son administration centrale dans l'Union, à moins que les décisions concernant les finalités et les moyens du traitement des données à caractère personnel ne soient prises dans un autre établissement du responsable du traitement dans l'Union. Dans ce cas, c'est cet établissement qui devrait être considéré comme l'établissement principal. L'établissement principal d'un responsable du traitement dans l'Union devrait être déterminé en fonction de critères objectifs et devrait supposer l'exercice effectif et réel d'activités de gestion déterminant les décisions principales quant aux finalités (…) et aux modalités du traitement dans le cadre d'une installation stable. Ce critère ne devrait pas dépendre du fait que le traitement ait effectivement lieu à cet endroit; la présence et l'utilisation de moyens techniques et de technologies permettant le traitement de données à caractère personnel ou la réalisation d'activités de ce type ne constituent pas en soi l'établissement principal ni, dès lors, un critère déterminant à cet égard. L'établissement principal du sous-traitant devrait être le lieu de son administration centrale dans l'Union et, s'il ne dispose pas d'une administration centrale dans l'Union, le lieu où se déroule l'essentiel des activités de traitement dans l'Union. Lorsque le responsable du traitement et le sous-traitant sont tous deux concernés, l'autorité de contrôle de l'État membre dans lequel le responsable du traitement a son établissement principal devrait rester l'autorité de contrôle chef de file, tandis que l'autorité de contrôle du sous-traitant devrait être considérée comme une autorité de contrôle concernée et devrait participer à la procédure de coopération prévue par le présent règlement. En tout état de cause, les autorités de contrôle de l'État membre ou des États membres dans lesquels le sous-traitant a un ou plusieurs établissements ne devraient pas être considérées comme des autorités de contrôle concernées lorsque le projet de décision ne concerne que le responsable du traitement.

Lorsque le traitement est effectué par un groupe d'entreprises, l'établissement principal de l'entreprise qui exerce le contrôle devrait être considéré comme l'établissement principal du groupe d'entreprises, excepté lorsque les finalités et les moyens du traitement sont déterminés par une autre entreprise.

(28) Un groupe d'entreprises devrait consister en une entreprise qui exerce le contrôle et des entreprises contrôlées, la première devant être celle qui peut exercer une influence dominante sur les autres du fait, par exemple, de la détention du capital, d'une participation financière ou des règles qui la régissent, ou du pouvoir de faire appliquer les règles relatives à la protection des données à caractère personnel. Une entreprise centrale qui contrôle le traitement de données à caractère personnel dans des entreprises qui lui sont affiliées forme avec ces dernières une entité qui peut être considérée comme un "groupe d'entreprises".

(29) Les données à caractère personnel relatives aux enfants (…) nécessitent une protection spécifique parce que ceux-ci peuvent être moins conscients des risques, des conséquences, des garanties et de leurs droits en matière de traitement des données. (...). Sont en particulier concernées l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et la collecte de données relatives aux enfants lors de l'utilisation de services fournis directement à un enfant.

(30) Tout traitement de données à caractère personnel devrait être licite et loyal. (…). Les personnes physiques devraient être informées en toute transparence que des données à caractère personnel les concernant sont collectées, utilisées, consultées ou traitées, et de la mesure dans laquelle ces données sont ou seront traitées. Le principe de transparence veut que toute information et communication relative au traitement de ces données soit aisément accessible et facile à comprendre, et formulée en termes simples et clairs. Cela vaut en particulier pour l'information des personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes concernées et celles relatives à leur droit d'obtenir la confirmation et la communication que des données à caractère personnel les concernant font l'objet d'un traitement. Les personnes physiques devraient être informées des risques, règles, garanties et droits relatifs au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en relation avec le traitement. En particulier, les finalités précises du traitement devraient être explicites et légitimes, et déterminées lors de la collecte des données. Les données devraient être adéquates et pertinentes (…) au regard des finalités pour lesquelles elles sont traitées, ce qui exige notamment de veiller à ce que les données collectées ne soient pas excessives et à ce que leur durée de conservation soit limitée au strict minimum. (…). Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement en vue de leur effacement ou d'une révision périodique.

Il y a lieu de prendre toutes les mesures raisonnables afin que les données à caractère personnel qui sont inexactes soient rectifiées ou effacées. Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, et notamment à prévenir l'accès non autorisé à ces données et à l'équipement servant à leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement.

(31) Pour être licite, le traitement devrait être fondé sur le consentement de la personne concernée ou sur tout autre fondement juridique légitime prévu par la législation, soit dans le présent règlement soit dans un autre acte législatif de l'Union ou d'un État membre, ainsi que le prévoit le présent règlement, compte tenu également de la nécessité de procéder au traitement pour respecter l'obligation légale à laquelle le responsable du traitement est soumis ou pour exécuter un contrat auquel la personne concernée est partie ou des mesures précontractuelles prises à la demande de celle-ci.

(31 *bis*) Lorsque le présent règlement fait référence à une base juridique ou à une mesure législative, il ne s'agit pas nécessairement d'un acte législatif adopté par un parlement, sans préjudice des obligations prévues par l'ordre constitutionnel de l'État membre concerné; cependant, cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, comme l'exige la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme.

(32) Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a bien consenti au traitement. En particulier, dans le contexte d'une déclaration écrite relative à une autre question, des garanties devraient faire en sorte que la personne concernée soit consciente du consentement donné et de sa portée. Une déclaration de consentement rédigée préalablement par le responsable du traitement devrait être fournie sous une forme intelligible et facilement accessible, en des termes clairs et simples, et son contenu ne devrait pas être inhabituel dans le contexte global. Pour que le consentement soit donné en connaissance de cause, la personne concernée devrait être informée au moins de l'identité du responsable du traitement et des finalités du traitement auquel sont destinées les données à caractère personnel; le consentement ne devrait pas être considéré comme libre si la personne concernée ne dispose pas d'une véritable liberté de choix et n'est pas en mesure de refuser ou de se rétracter sans subir de préjudice.

(33) (...)

(34) Pour garantir que le consentement a été donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement et que ce déséquilibre fait douter que le consentement ait été donné librement dans tous les cas de figure de cette situation particulière. Le consentement est présumé ne pas être libre si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données bien que ce consentement soit opportun dans le cas individuel, ou si l'exécution d'un contrat dépend du consentement sans que cela soit nécessaire et que la personne concernée ne peut pas raisonnablement obtenir de services équivalents auprès d'une autre source sans consentement.

(35) Le traitement devrait être licite lorsqu'il est nécessaire dans le cadre d'un contrat ou de la conclusion envisagée d'un contrat.

(35 *bis*) Le présent règlement énonce des règles générales relatives à la protection des données et prévoit que, dans certains cas spécifiques, les États membres sont également habilités à édicter des règles nationales en matière de protection des données. Le présent règlement n'exclut donc pas les législations nationales qui définissent les circonstances de situations particulières de traitement, notamment en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite. La législation nationale peut également prévoir des conditions spéciales de traitement pour certains secteurs ainsi que pour le traitement de catégories particulières de données.

(36) Lorsque le traitement est réalisé conformément à une obligation légale à laquelle est soumis le responsable du traitement, ou lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt général ou relevant de l'exercice de l'autorité publique, le traitement devrait avoir son fondement (…) dans le droit de l'Union ou dans la législation nationale d'un État membre. (...). Il devrait appartenir également au droit de l'Union ou à la loi nationale de déterminer la finalité du traitement. En outre, cette base pourrait (...) préciser les conditions générales du règlement régissant la licéité du traitement des données, définir les spécifications relatives au responsable du traitement, au type de données faisant l'objet du traitement, aux personnes concernées, aux entités auxquelles les données peuvent être communiquées, aux limitations de la finalité, à la durée de conservation et à d'autres mesures visant à garantir un traitement licite et loyal.

Il devrait appartenir également au droit de l'Union ou à la législation nationale de déterminer si le responsable du traitement investi d'une mission d'intérêt général ou relevant de l'exercice de l'autorité publique doit être une autorité publique ou une autre personne physique ou morale de droit public ou de droit privé, telle qu'une association professionnelle, dans le cas où des raisons d'intérêt général le justifient, et notamment à des fins de santé publique, en ce compris la protection de la santé, la protection sociale et la gestion des services de santé.

(37) Le traitement de données à caractère personnel devrait être également considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou d'une autre personne. (...). Certains types de *traitement des données peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des* fins humanitaires, notamment afin de *suivre une épidémie et sa propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle*.

(38) Les intérêts légitimes d'un responsable du traitement, y compris un responsable du traitement auquel les données peuvent être communiquées, ou d'un tiers peuvent constituer un fondement juridique au traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée. Un intérêt légitime pourrait notamment exister lorsqu'il y a un lien pertinent et approprié entre la personne concernée et le responsable du traitement, par exemple si la personne concernée est cliente de celui-ci ou si elle est à son service. (...) En tout état de cause, l'existence d'un intérêt légitime mérite un examen attentif, notamment afin de déterminer si une personne concernée peut s'attendre, au moment et dans le cadre de la collecte des données, à ce que celles-ci fassent l'objet d'un traitement à cette fin. Cet examen doit en particulier tenir compte du fait que la personne concernée est ou non un enfant, cette catégorie de personnes nécessitant en effet une protection spécifique.
La personne concernée devrait pouvoir s'opposer au traitement des données la concernant, pour des raisons tenant à sa situation personnelle, et ce, gratuitement. Afin d'assurer la transparence, le responsable du traitement devrait être tenu d'informer expressément la personne concernée des intérêts légitimes poursuivis, et de justifier ces derniers, ainsi que du droit de la personne de s'opposer au traitement. (...)

(38 *bis*) Les responsables du traitement qui font partie d'un groupe d'entreprises ou d'un établissement affilié à un organisme central peuvent avoir un intérêt légitime à transmettre des données à caractère personnel au sein du groupe d'entreprises à des fins administratives internes, y compris le traitement de données à caractère personnel relatives à des clients ou des salariés. Les principes généraux régissant le transfert de données à caractère personnel**,** au sein d'un groupe d'entreprises, à une entreprise située dans un pays tiers (…) ne sont pas remis en cause.

(39) Le traitement de données dans la mesure strictement nécessaire aux fins de garantir la sécurité du réseau et des informations, c'est-à-dire la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées ou transmises, ainsi que la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par les pouvoirs publics, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes de réaction aux incidents touchant la sécurité informatique (CSIRT), des fournisseurs de réseaux ou de services de communications électroniques, et des fournisseurs de technologies et services de sécurité, constitue un intérêt légitime du responsable du traitement *concerné*. Il pourrait s'agir, par exemple, d'empêcher l'accès non autorisé à des réseaux de communications électroniques et la distribution de codes malveillants, et de faire cesser des attaques par "déni de service" et des dommages touchant les systèmes de communications informatiques et électroniques. Le traitement de données à caractère personnel strictement nécessaire à des fins de prévention de la fraude constitue également un intérêt légitime du responsable du traitement concerné. Le traitement de données à caractère personnel à des fins de marketing direct peut être considéré comme répondant à un intérêt légitime.

(40) Le traitement des données à caractère personnel à d'autres fins que les finalités de la collecte initiale des données ne devrait être autorisé que s'il est compatible avec lesdites finalités. Dans ce cas, aucune base juridique distincte autre que celle qui a permis la collecte des données n'est requise. (…) Si le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, le droit de l'Union ou la législation d'un État membre peut déterminer et préciser les missions et les fins pour lesquelles le traitement ultérieur est considéré comme licite. Le traitement ultérieur (…) à des fins d'archivage dans l'intérêt public, à des fins statistiques, scientifiques ou historiques (…) ou en vue d'un règlement futur des litiges devrait être considéré comme un traitement licite compatible. La base juridique prévue par le droit de l'Union ou par la législation nationale en ce qui concerne la collecte et le traitement de données à caractère personnel peut également être utilisée pour un traitement ultérieur à d'autres fins si celles-ci sont conformes à la mission et si le responsable du traitement est en droit de collecter les données à ces autres fins.

Afin de vérifier si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les conditions de licéité du traitement initial, devrait tenir compte **entre autres** de l'existence éventuelle de tout lien entre ces finalités et les finalités du traitement ultérieur envisagé, du contexte dans lequel les données ont été collectées, y compris les attentes raisonnables de la personne concernée quant à leur utilisation ultérieure, de la nature des données à caractère personnel, des conséquences pour les personnes concernées du traitement ultérieur envisagé et de l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement envisagé. Lorsque l'autre finalité envisagée n'est pas compatible avec la finalité initiale de la collecte des données, il convient que le responsable du traitement obtienne le consentement de la personne concernée à cette autre finalité ou qu'il fonde le traitement sur un autre motif légitime, en particulier lorsque le droit de l'Union ou la législation de l'État membre dont relève le responsable des données le prévoit. (…).

En tout état de cause, l'application des principes énoncés par le présent règlement et, en particulier, l'information de la personne concernée au sujet de ces autres finalités et de ses droits (…), y compris son droit à s'opposer au traitement, devraient être assurées. (…). Le fait, pour le responsable du traitement, de révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre ces données à une autorité compétente devrait être considéré comme relevant de l'intérêt légitime du responsable du traitement. Néanmoins, cette transmission dans l'intérêt légitime du contrôleur ou le traitement ultérieur des données à caractère personnel devrait être interdit lorsque le traitement est incompatible avec une obligation de confidentialité de nature juridique, professionnelle ou autre.

(41) Les données à caractère personnel qui sont, par nature, particulièrement sensibles (…) du point de vue des droits et des libertés fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées peut entraîner des risques importants pour les droits et libertés fondamentaux. Devraient en faire partie les données à caractère personnel qui révèlent l'origine raciale ou ethnique, étant entendu que l'utilisation de l'expression "origine raciale" dans le présent règlement n'implique pas que l'Union européenne adhère à des théories visant à établir l'existence de races humaines distinctes. Ces données ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne soit autorisé dans les cas spécifiques prévus par le présent règlement, compte tenu du fait que la législation des États membres peut prévoir des dispositions spécifiques relatives à la protection des données afin d'adapter l'application des règles prévues par le présent règlement en ce qui concerne le respect d'une obligation légale ou l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Outre les exigences spécifiques de ce traitement, les principes généraux et les autres dispositions du présent règlement devraient être applicables, en particulier en ce qui concerne les conditions de licéité du traitement.
Des dérogations à l'interdiction générale de traitement de ces catégories particulières de données à caractère personnel devraient être explicitement prévues, notamment si la personne concernée donne son consentement explicite ou pour tenir compte de besoins spécifiques, en particulier lorsque le traitement a lieu dans le cadre d'activités légitimes de certaines associations ou fondations ayant pour finalité de permettre l'exercice des libertés fondamentales.

Des catégories particulières de données à caractère personnel peuvent également faire l'objet d'un traitement lorsque les données ont été manifestement rendues publiques ou ont été transférées, volontairement et à la demande de la personne concernée, au responsable du traitement à une fin particulière précisée par la personne concernée, lorsque le traitement est effectué dans l'intérêt de la personne concernée.

Le droit des États membres et celui de l'Union peuvent prévoir que l'interdiction générale de traitement de ces catégories particulières de données à caractère personnel dans certains cas ne peut pas être levée par le consentement explicite de la personne concernée.

(42) Des dérogations à l'interdiction du traitement des catégories de données sensibles devraient également être autorisées si la législation de l'Union ou des États membres le permet, et sous réserve de garanties appropriées, afin de protéger les données à caractère personnel et d'autres droits fondamentaux, dans le cas où (...) des raisons d'intérêt public le justifient, notamment *le traitement des données* en matière de droit du travail, de la sécurité et de la protection sociales, y compris les retraites, et *à des fins de sécurité sanitaire, de surveillance et d'alerte, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé, ou en vue de garantir des normes élevées de qualité et de sécurité des soins et des services de santé et des produits pharmaceutiques ou des appareils médicaux, ou d'évaluer les politiques publiques menées dans le domaine de la santé, notamment par la production d'indicateurs de qualité et d'activité.*

Cela peut être fait à des fins de santé, en ce compris la santé publique (...) et la gestion des services de santé, notamment pour assurer la qualité et la rentabilité des procédures de règlement des demandes de remboursement et de services dans le régime d'assurance-maladie, à des fins d'archivage dans l'intérêt public, ou à des fins historiques, statistiques et (…) scientifiques.

Une dérogation permettrait en outre de traiter ces données, si nécessaire, aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice, que ce soit dans le cadre d'une procédure judiciaire, administrative ou extrajudiciaire.

(42 *bis*) *Les catégories particulières de données à caractère personnel qui nécessitent une protection plus élevée peuvent être traitées uniquement à des fins sanitaires, si nécessaire, afin d'atteindre ces objectifs dans l'intérêt des personnes et de la société dans son ensemble, notamment dans le cadre de la gestion des services et des systèmes de soins de santé ou d'aide sociale*, y compris le traitement, par les autorités de gestion et les autorités centrales nationales de santé, de ces données, en vue du contrôle de la qualité, de l'information des gestionnaires et de la supervision générale nationale et locale du système de soins de santé ou d'aide sociale *et en vue d'assurer la continuité des soins de santé ou des services sociaux et des soins de santé transnationaux ou la sécurité sanitaire, à des fins de surveillance et d'alerte ou à des fins d'archivage dans l'intérêt public, à des fins historiques, statistiques ou scientifiques, ainsi que pour des études menées dans l'intérêt public dans le domaine de la santé publique. Le présent règlement devrait donc prévoir des conditions harmonisées pour le traitement des catégories particulières de données à caractère personnel relatives à la santé, pour répondre à des besoins spécifiques, en particulier lorsque le traitement de ces données est effectué à certaines fins relatives à la santé par des personnes soumises à une obligation de secret professionnel (...). Le droit de l'Union ou la législation nationale devrait prévoir des mesures spécifiques et appropriées afin de protéger les droits fondamentaux et les données à caractère personnel des personnes physiques. (...).*

(*42 ter) Le traitement des catégories particulières de données à caractère personnel (...) peut être nécessaire pour des raisons d'intérêt public dans les domaines de la santé publique, et sans le consentement de la personne concernée. Ce traitement est subordonné à des mesures appropriées et spécifiques visant à protéger les droits et les libertés des personnes. Dans ce contexte, la notion de "santé publique" s'interprète selon la définition prévue dans le règlement (CE) n° 1338/2008 du Parlement européen et du Conseil du 16 décembre 2008 relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail, et désigne l'ensemble des éléments liés à la santé, à savoir, l'état de santé, y compris le décès et le handicap, les éléments déterminant cet état de santé, les besoins en soins de santé, les ressources allouées aux soins de santé, l'offre de soin et l'accès universel à ces soins ainsi que les dépenses et le financement des soins de santé et les causes de décès.*
Ces traitements de données à caractère personnel concernant la santé autorisés pour des motifs d'intérêt public ne doivent pas aboutir à ce que ces données soient traitées à d'autres fins par des tiers, tels que les employeurs, les compagnies d'assurance et les banques.

(43) En outre, le traitement de données à caractère personnel par des autorités publiques en vue de réaliser les objectifs, prévus par le droit constitutionnel ou le droit international public, d'associations à caractère religieux officiellement reconnues est effectué pour des raisons d'intérêt public.

(44) Si, dans le cadre d'activités liées à des élections, le fonctionnement du système démocratique suppose, dans un État membre, que les partis politiques collectent des données relatives aux opinions politiques des personnes, le traitement de telles données peut être autorisé pour des motifs d'intérêt public, à condition que des garanties appropriées soient prévues.

(45) Si les données qu'il traite ne lui permettent pas d'identifier une personne physique, (...) le responsable du traitement ne devrait pas être tenu d'obtenir des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter une disposition du présent règlement. (...). Toutefois, le responsable du traitement ne devrait pas refuser des informations supplémentaires fournies par la personne concernée afin de faciliter l'exercice de ses droits.

(46) Le principe de transparence veut que toute information adressée au public ou à la personne concernée soit aisément accessible et facile à comprendre, formulée en termes simples et clairs et en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels. Ces informations peuvent être fournies également sous forme électronique, comme par exemple via un site internet lorsqu'elles s'adressent au public. Ceci vaut tout particulièrement lorsque, dans des domaines tels que la publicité en ligne, la multiplication des acteurs et la complexité des technologies utilisées empêchent la personne concernée de savoir exactement si des données à caractère personnel la concernant sont collectées, par qui et dans quel but. Les enfants nécessitant une protection spécifique, toute information et communication, lorsque le traitement des données les concerne (…), devrait être rédigée en des termes simples et clairs que l'enfant peut aisément comprendre.

(47) Des modalités devraient être prévues pour faciliter l'exercice, par la personne concernée, des droits qui lui sont conférés par le présent règlement, notamment les moyens de demander (…) l'accès aux données, leur rectification ou leur effacement, et d'exercer son droit d'opposition. Le responsable du traitement devrait donc également fournir les moyens d'effectuer des demandes par voie électronique, notamment lorsque les données à caractère personnel font l'objet d'un traitement automatisé. Le responsable du traitement devrait être tenu de répondre à la personne concernée sans tarder et au plus tard dans un délai d'un mois et de motiver toute intention de ne pas accéder à sa demande.

Toutefois, si les demandes sont manifestement infondées ou excessives, par exemple lorsque la personne concernée présente de façon répétée des demandes d'information déraisonnables ou fait une utilisation abusive de son droit à l'information, par exemple en fournissant des informations fausses ou trompeuses dans le cadre de sa demande, le responsable du traitement pourrait refuser de donner suite à la demande.

(48) Le principe de traitement loyal et transparent exige que la personne concernée soit informée (…) de l'existence du traitement et de ses finalités (…). Le responsable du traitement devrait fournir à la personne concernée toute autre information nécessaire pour assurer un traitement loyal et transparent. En outre, la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci. Lorsque les données sont collectées auprès de la personne concernée, il importe que celle-ci sache également si elle est obligée de fournir ces informations et à quelles conséquences elle s'expose si elle ne les fournit pas.

(49) L'information sur le traitement des données à caractère personnel devrait être donnée à la personne concernée au moment où ces données sont recueillies ou, si la collecte des données n'a pas lieu auprès de la personne concernée, dans un délai raisonnable en fonction des circonstances propres à chaque cas. Lorsque des données peuvent être légitimement communiquées à un autre destinataire, il convient que la personne concernée soit informée lorsque ces données sont communiquées pour la première fois audit destinataire. Lorsqu'il a l'intention de traiter les données à des fins autres que la finalité initiale de la collecte des données, le responsable du traitement devrait au préalable fournir à la personne concernée des informations au sujet de cette autre finalité et toute autre information nécessaire. Lorsque l'origine des données n'a pas pu être communiquée à la personne concernée parce que plusieurs sources ont été utilisées, ces informations devraient être fournies d'une manière générale.

(50) Toutefois, il n'est pas nécessaire d'imposer cette obligation si la personne concernée dispose déjà de cette information, ou si l'enregistrement ou la divulgation des données sont expressément prévus par la loi, ou si l'information de la personne concernée se révèle impossible ou exige des efforts disproportionnés. Tel pourrait être le cas, en particulier, des traitements à des fins d'archivage dans l'intérêt public, à des fins historiques, statistiques ou (…) scientifiques; à cet égard, peuvent être pris en considération le nombre de personnes concernées, l'ancienneté des données, ainsi que les garanties appropriées éventuelles adoptées.

(51) Une personne physique devrait avoir le droit d'accéder aux données qui ont été collectées à son sujet et d'exercer ce droit facilement, à des intervalles raisonnables, afin de s'informer du traitement dont elle fait l'objet et d'en vérifier la licéité. *Cela inclut le droit des personnes d'accéder aux données ayant trait à leur santé, par exemple les données des dossiers médicaux faisant état de diagnostics, de résultats d'examens, d'avis de médecins traitants ou de tout traitement ou intervention effectués.* En conséquence, chaque personne concernée devrait avoir le droit de connaître et de se faire communiquer, en particulier, la finalité du traitement des données, le cas échéant la durée de leur conservation, l'identité des destinataires, la logique qui sous-tend leur éventuel traitement automatisé et les conséquences qu'il pourrait avoir, au moins en cas de profilage. Ce droit ne devrait pas porter atteinte aux droits et libertés d'autrui, notamment au secret des affaires, ni à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Toutefois, ces considérations ne sauraient aboutir au refus de toute information de la personne concernée. Lorsque le responsable du traitement traite une grande quantité de données relatives à la personne concernée, il peut demander à celle-ci de préciser, avant de lui fournir les informations, sur quelles données ou quelles opérations de traitement sa demande porte.

(52) Le responsable du traitement devrait prendre toutes les mesures raisonnables afin de s'assurer de l'identité d'une personne concernée demandant l'accès aux données, en particulier dans le contexte des services et identifiants en ligne. (...) L'identification devrait comprendre l'identification numérique d'une personne concernée, par exemple au moyen d'un mécanisme d'authentification tel que les justificatifs d'identité utilisés par la personne concernée pour se connecter au service en ligne proposé par le responsable du traitement des données. Un responsable des données ne devrait pas conserver des données à caractère personnel à la seule fin d'être en mesure de réagir à d'éventuelles demandes.

(53) Une personne physique devrait avoir le droit de faire rectifier des données à caractère personnel la concernant, et disposer d'un "droit à l'oubli numérique" lorsque la conservation de ces données n'est pas conforme au présent règlement ou au droit de l'Union ou des États membres auquel le responsable du traitement est soumis. En particulier, les personnes concernées devraient avoir le droit d'obtenir que leurs données soient effacées et ne soient plus traitées, lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été recueillies ou traitées, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de données à caractère personnel les concernant, ou encore lorsque le traitement de leurs données à caractère personnel n'est pas conforme au présent règlement. Ce droit est en particulier important lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et donc mal informée des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'internet. La personne concernée devrait pouvoir exercer ce droit nonobstant le fait qu'elle n'a plus le statut d'enfant. Toutefois, la conservation des données devrait être licite [...] lorsqu'elle est nécessaire à *l'exercice du droit à la liberté d'expression* et d'information, au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou à l'exercice de l'autorité publique dont est investi le responsable du traitement, *pour des motifs d'intérêt général dans le domaine de la santé publique*, à des fins d'archivage d'intérêt général, à des fins historiques, statistiques et scientifiques (...) ou à la constatation, à l'exercice ou à la défense de droits en justice.

(54) Afin de renforcer le "droit à l'oubli numérique" dans l'environnement en ligne, le droit à l'effacement des données devrait en outre être étendu de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques soit tenu d'informer les responsables du traitement qui traitent lesdites données **(...)** d'effacer tout lien vers ces données, ou toute copie ou reproduction de celles-ci.

Pour s'acquitter de l'obligation d'information susvisée, le responsable du traitement devrait prendre (…) des mesures raisonnables, compte tenu des technologies existantes et des moyens dont il dispose, y compris des mesures techniques, en ce qui concerne les données publiées sous sa responsabilité. (...).

(54 *bis*) Les méthodes visant à limiter le traitement de données à caractère personnel pourraient consister, entre autres, à déplacer temporairement les données sélectionnées vers un autre système de traitement, à rendre les données sélectionnées inaccessibles aux utilisateurs ou à retirer temporairement les données publiées d'un site internet. Dans les systèmes de fichiers automatisés, la limitation du traitement de données à caractère personnel devrait en principe être assurée par des moyens techniques; le fait que le traitement des données à caractère personnel est limité devrait être indiqué de manière à apparaître clairement dans le système.

(55) Pour leur permettre de mieux maîtriser encore l'utilisation qui est faite des données les concernant (...), les personnes concernées devraient avoir le droit, lorsque des données à caractère personnel font l'objet d'un traitement automatisé, de recevoir les données les concernant qu'elles ont communiquées au responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et les communiquer à un autre responsable du traitement.

Ce droit devrait s'appliquer lorsque la personne concernée a fourni les données à caractère personnel en donnant son consentement ou dans le cadre de l'exécution d'un contrat. Il ne devrait pas s'appliquer lorsque le traitement est fondé sur un motif légal autre que le consentement ou l'exécution d'un contrat. De par sa nature même, ce droit ne devrait pas être exercé à l'encontre de responsables du traitement des données dans l'exercice de leurs fonctions publiques. Il ne devrait donc pas s'appliquer, en particulier, lorsque le traitement de données à caractère personnel est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Le droit de la personne concernée de transmettre des données à caractère personnel ne crée pas, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement des données qui soient techniquement compatibles.

Lorsqu'un ensemble de données à caractère personnel concerne plusieurs personnes, le droit de transmettre les données devrait s'entendre sans préjudice des conditions de licéité du traitement des données à caractère personnel relatives à une autre personne concernée conformément au présent règlement. Ce droit ne devrait pas non plus porter atteinte au droit de la personne concernée d'obtenir l'effacement des données à caractère personnel ni aux limitations de ce droit fixées dans le présent règlement et, plus particulièrement, il ne devrait pas entraîner l'effacement des données à caractère personnel qui ont été fournies par la personne concernée pour l'exécution d'un contrat, dans la mesure et aussi longtemps que ces données sont nécessaires à l'exécution de ce contrat. (...)

(56) Dans les cas où des données à caractère personnel pourraient faire l'objet d'un traitement licite (…) parce que le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou sur la base des intérêts légitimes du responsable du traitement ou d'un tiers, toute personne concernée devrait néanmoins avoir le droit de s'opposer au traitement de toute donnée en rapport avec sa situation personnelle. Il devrait incomber au responsable du traitement de prouver que ses intérêts légitimes impérieux prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée.

(57) Lorsque des données à caractère personnel sont traitées à des fins de marketing direct, la personne concernée devrait avoir le droit de s'opposer à ce traitement, qu'il s'agisse d'un traitement initial ou postérieur, sans frais et d'une manière simple et effective.

(58) La personne concernée devrait avoir le droit de ne pas faire l'objet d'une décision impliquant l'évaluation de certains aspects personnels la concernant, qui résulterait exclusivement d'un traitement automatisé et *qui produirait des effets juridiques la concernant* ou qui l'affecterait de manière sensible, par exemple le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine. Ce type de traitement inclut notamment le "profilage", à savoir toute forme de traitement automatisé de données à caractère personnel visant à évaluer certains aspects personnels liés à une personne physique, notamment par l'analyse et la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles ou les intérêts, la fiabilité ou le comportement, ou la localisation et les déplacements, dès lors qu'il produit des effets juridiques la concernant ou qu'il l'affecte de manière sensible [...]. Toutefois, la prise de décision fondée sur un tel traitement, y compris le profilage, devrait être permise lorsqu'elle est expressément autorisée par le droit de l'Union ou la législation d'un État membre auquel le responsable du traitement est soumis, entre autres, aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale et d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement, ou nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, ou si la personne concernée y a donné son consentement explicite. En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, y compris une information spécifique de la personne concernée et le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision. Afin d'assurer à la personne concernée un traitement équitable et transparent des données la concernant, eu égard aux circonstances particulières et au contexte dans lesquels ces données sont traitées, le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer sur le plan technique et au niveau de l'organisation les mesures nécessaires pour faire en sorte, en particulier, que les facteurs qui entraînent des erreurs dans les données soient corrigés et que les risques d'erreur soient réduits au minimum, et sécuriser les données à caractère personnel de façon à tenir compte des risques susceptibles de peser sur les intérêts et les droits de la personne concernée et à prévenir, notamment, les discriminations à l'égard des personnes physiques fondées sur la race ou l'origine ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou la santé, ou encore l'orientation sexuelle, ou qui se traduisent par des mesures produisant un tel effet. La prise de décision et le profilage automatisés fondés sur des catégories particulières de données à caractère personnel ne devraient être autorisés que dans des conditions spécifiques.

(58 *bis*) Le profilage en tant que tel est soumis aux dispositions (générales) du présent règlement régissant le traitement des données à caractère personnel (fondement juridique du traitement, principes en matière de protection des données, etc.) et s'accompagne de garanties spécifiques (par exemple, l'obligation de réaliser une analyse d'impact dans certains cas, ou les dispositions prévoyant que des informations spécifiques soient fournies à la personne concernée). Le comité européen de la protection des données devrait avoir la possibilité de formuler des orientations à cet égard.

(59) Des limitations des principes spécifiques et du droit à l'information, du droit d'accès, de rectification et d'effacement, ou du droit à la portabilité des données, du droit d'opposition, des mesures fondées sur le profilage, ainsi que de la communication d'une violation des données à caractère personnel à une personne concernée, et des limitations de certaines obligations connexes des responsables du traitement des données peuvent être imposées par le droit de l'Union ou d'un État membre, dans la mesure strictement nécessaire et proportionnée dans une société démocratique, pour garantir la sécurité publique, notamment aux fins de la protection de la vie humaine en cas, plus particulièrement, de catastrophe d'origine naturelle ou humaine, aux fins de la prévention, de l'enquête et des poursuites dans le cadre d'infractions pénales ou de manquements à la déontologie des professions réglementées, aux fins d'autres intérêts généraux, y compris d'un intérêt économique ou financier important, de l'Union ou d'un État membre, aux fins de la tenue de registres publics conservés pour des motifs d'intérêt général, aux fins du traitement ultérieur de données à caractère personnel archivées pour fournir des informations précises relatives au comportement politique dans le cadre des régimes des anciens États totalitaires ou aux fins de la protection de la personne concernée ou des droits ou libertés de tiers, y compris la protection sociale, la santé publique et les finalités humanitaires, par exemple l'exécution d'une mission dont est chargé le Mouvement international de la Croix-Rouge et du Croissant-Rouge (...). Ces limitations doivent être conformes aux exigences énoncées par la charte des droits fondamentaux de l'Union européenne et par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

(59 *bis*) Aucune disposition du présent règlement ne devrait déroger (...) au privilège de non-divulgation des informations confidentielles du Mouvement international de la Croix-Rouge et du Croissant-Rouge en droit international, qui est applicable dans les procédures judiciaires et administratives. (...)

(60) Il y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. Il importe en particulier que le responsable du traitement (…) soit tenu de mettre en œuvre les mesures appropriées et soit à même (…) de démontrer la conformité (…) des activités de traitement au présent règlement (...). Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités des traitements ainsi que du risque que ceux-ci présentent pour les droits et les libertés des personnes physiques.

(60 *bis*) Ces risques, aux degrés de probabilité et de gravité variables, peuvent apparaître lorsque les traitements de données sont susceptibles d'entraîner des dommages physiques, matériels ou moraux, en particulier lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important; ou lorsque les personnes concernées sont susceptibles d'être privées de leurs droits et libertés ou de la maîtrise de l'utilisation qui est faite de leurs données à caractère personnel; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances philosophiques, l'appartenance syndicale, ainsi que des données génétiques ou concernant la santé ou la vie sexuelle ou des données relatives à des condamnations ou à des infractions pénales, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse et de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles ou les intérêts, la fiabilité ou le comportement, ou la localisation et les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes vulnérables, en particulier des enfants; lorsque le traitement porte sur un volume important de données à caractère personnel et sur un nombre important de personnes concernées; (...).

60 *ter*) *Il convient de déterminer la probabilité et la gravité du risque en fonction de la nature, de la portée, du contexte et des finalités du traitement de données. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque élevé. On entend par risque élevé un risque particulier de porter atteinte aux droits et aux libertés des personnes physiques* (...).

60 *quater*) Les directives relatives à la mise en œuvre de mesures appropriées par le responsable du traitement ou le sous-traitant et à la démonstration de la conformité de ses activités, notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et les meilleures pratiques visant à atténuer le risque, pourraient être fournies notamment au moyen de codes de conduite et de certifications approuvés et de lignes directrices du comité européen de la protection des données, ou au moyen des indications données par un délégué à la protection des données. Le comité européen de la protection des données peut également publier des lignes directrices relatives aux opérations de traitement considérées comme peu susceptibles de présenter un risque élevé pour les droits et libertés des personnes physiques et indiquer les mesures qui peuvent suffire dans de tels cas pour faire face à un tel risque. (...)

(61) La protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel nécessite de prendre les mesures techniques et organisationnelles appropriées, de sorte que les exigences du présent règlement soient respectées. Afin d'être en mesure de démontrer la conformité au présent règlement, le responsable du traitement devrait adopter des règles internes et appliquer des mesures appropriées, qui répondent en particulier aux principes de la protection des données dès la conception et de la protection des données par défaut. Ces mesures devraient consister notamment à limiter le traitement des données à caractère personnel, (...) à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de superviser le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer. Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui se fondent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il conviendrait d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état d'avancement de la technique, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données.

(62) La protection des droits et libertés des personnes concernées, de même que la responsabilité des responsables du traitement et de leurs sous-traitants, y compris dans le cadre de la surveillance exercée par les autorités de contrôle et des mesures prises par elles, exige une répartition claire des responsabilités au titre du présent règlement, notamment dans le cas où le responsable du traitement détermine les finalités (…) et les moyens du traitement conjointement avec d'autres responsables, ou lorsqu'un traitement est effectué pour le compte d'un responsable du traitement.

(63) Lorsqu'un responsable du traitement qui n'est pas établi dans l'Union traite des données à caractère personnel concernant des personnes résidant dans l'Union, et que les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, ou à l'observation de leur comportement dans l'Union, (...) il conviendrait que le responsable du traitement désigne un représentant, à moins que (...) *le traitement qu'il effectue soit* occasionnel et *peu susceptible de constituer un risque pour les droits et libertés des personnes concernées, compte tenu de la nature, de la portée, du contexte et des finalités du traitement,* ou que le responsable du traitement ne soit une autorité ou un organisme public (…). Le représentant devrait agir pour le compte du responsable du traitement et devrait pouvoir être contacté par toute autorité de contrôle. Le représentant devrait être expressément désigné par un mandat écrit du responsable du traitement le chargeant d'agir en son nom pour remplir les obligations qui lui incombent en vertu du présent règlement. La désignation de ce représentant ne modifie pas la responsabilité du responsable du traitement au titre du présent règlement.
Ce représentant devrait accomplir ses tâches conformément au mandat reçu du responsable du traitement, y compris en ce qui concerne la coopération avec les autorités de contrôle compétentes pour toute action visant à se conformer au présent règlement. Le représentant désigné devrait faire l'objet de mesures coercitives en cas de non-respect du présent règlement par le responsable du traitement.

(63 *bis*) Afin que les prescriptions du présent règlement soient respectées dans le cadre d'un traitement réalisé par un sous-traitant pour le compte du responsable du traitement, lorsque ce dernier confie des opérations de traitement à un sous-traitant, il ne devrait faire appel qu'à des sous-traitants présentant des garanties suffisantes, notamment en termes de connaissances spécialisées, de fiabilité et de ressources, pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont aux prescriptions du présent règlement, y compris en matière de sécurité du traitement. (...) L'adhésion du sous-traitant à un code de conduite approuvé ou un mécanisme de certification approuvé peuvent être utilisés comme moyen de démontrer le respect des obligations incombant au responsable du traitement. La réalisation d'un traitement par un sous-traitant devrait être régie par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre liant le sous-traitant au responsable du traitement, définissant l'objet et la durée du traitement, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et tenant compte des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer, ainsi que du risque au regard des droits et des libertés de la personne concernée.

Le responsable du traitement et le sous-traitant peuvent choisir de recourir à un contrat particulier ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par une autorité de contrôle conformément au mécanisme de contrôle de la cohérence puis par la Commission, ou qui font partie d'une certification délivrée dans le cadre du mécanisme de certification. Après l'exécution du traitement pour le compte du responsable du traitement, le sous-traitant devrait renvoyer ou supprimer les données à caractère personnel, à moins que le droit de l'Union ou celui de l'État membre auquel le sous-traitant est soumis exige la conservation des données.

(64) (...)

(65) Afin d'apporter la preuve qu'il se conforme au présent règlement, le responsable du traitement ou le sous-traitant devrait tenir des registres pour toutes les catégories d'activités de traitement relevant de sa responsabilité. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à sa disposition sur demande pour qu'ils servent au contrôle des opérations en question.

(66) Afin de préserver la sécurité et de prévenir tout traitement contraire au présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques (...) inhérents au traitement et prenne des mesures pour les atténuer. Ces mesures devraient assurer un niveau de sécurité approprié, y compris en ce qui concerne la confidentialité, compte tenu, d'une part, des technologies disponibles et des coûts de mise en œuvre et, d'autre part, du risque lié au traitement de données à caractère personnel et de la nature des données à protéger. (…). Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient d'apprécier les risques que présente le traitement de données, tels que la destruction, la perte, l'altération, accidentelles ou illicites, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière, qui sont susceptibles d'entraîner des dommages physiques, matériels ou moraux.

(66 *bis*) Afin de mieux garantir le respect du présent règlement dans les cas où les traitements sont susceptibles de comporter un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque. Il convient de tenir compte du résultat de l'évaluation pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel est effectué dans le respect du présent règlement. Lorsqu'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il convient que l'autorité de contrôle soit consultée avant que le traitement n'ait lieu.

(67) Une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou moraux tels qu'une perte de maîtrise de leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social. (…). En conséquence, dès que le responsable du traitement apprend qu'une (…) violation de données à caractère personnel susceptible de causer des (...) dommages physiques, matériels ou moraux s'est produite, il conviendrait qu'il en informe l'autorité de contrôle sans retard injustifié et, lorsque c'est possible, dans les 72 heures. Si ce délai ne peut être respecté, la notification devrait être assortie d'une explication concernant ce retard. Les personnes physiques dont les droits et libertés pourraient être gravement affectés par la violation devraient en être averties sans retard injustifié afin qu'elles puissent prendre les précautions qui s'imposent. (…) La notification devra décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne concernée afin d'atténuer les effets négatifs pouvant découler de ladite violation. Il convient que les notifications aux personnes concernées soient effectuées aussi rapidement que possible, en coopération étroite avec l'autorité de contrôle et dans le respect des directives fournies par celle-ci ou par d'autres autorités compétentes (telles que les autorités répressives). Par exemple, vu la nécessité d'atténuer un risque immédiat de dommage, il faudrait adresser rapidement une notification aux personnes concernées, mais la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données ou la survenance de violations similaires pourrait justifier un délai plus long.

(68) (…) Il faut vérifier si toutes les mesures de protection technologiques et d'organisation appropriées ont été mises en œuvre pour établir immédiatement si une violation des données est intervenue et pour informer rapidement l'autorité de contrôle et la personne concernée (...). Il convient d'établir que la notification a été faite sans retard injustifié, compte tenu en particulier de la nature et de la gravité de la violation des données et de ses conséquences et effets néfastes pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir, dans le cadre des missions et des pouvoirs qui lui sont confiés par le présent règlement.

(68 *bis*) La communication à la personne concernée d'une violation de ses données à caractère personnel n'est pas nécessaire si le responsable du traitement a mis en œuvre les mesures de protection technologiques appropriées et si ces dernières ont été appliquées aux données concernées par ladite violation. Ces mesures de protection technologiques devraient inclure celles qui rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès, notamment en cryptant les données à caractère personnel (...).

(69) Lors de la fixation de règles détaillées concernant la forme et les procédures applicables à la notification des violations de données à caractère personnel, il convient de tenir dûment compte des circonstances de la violation, notamment du fait que les données à caractère personnel étaient ou non protégées par des mesures de protection techniques appropriées limitant efficacement le risque d'usurpation d'identité ou d'autres formes d'abus. Par ailleurs, ces règles et procédures devraient tenir compte des intérêts légitimes des autorités répressives dans les cas où une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances de la violation.

(70) La directive 95/46/CE prévoyait une obligation générale de notifier les traitements de données à caractère personnel aux autorités de contrôle. Or cette obligation génère une charge administrative et financière, sans pour autant avoir véritablement amélioré la protection des données. En conséquence, les obligations générales de notification devraient être supprimées et remplacées par des procédures et des mécanismes efficaces ciblant plutôt les types de traitement susceptibles de donner lieu à un risque élevé pour les droits et libertés de personnes physiques, du fait de leur nature, portée, *contexte* et finalités (…). On peut entendre par de tels types de traitement ceux qui, en particulier, passent par le recours aux nouvelles technologies, ou qui sont nouveaux et pour lesquels aucune analyse d'impact relative à la protection des données n'a été effectuée au préalable par le responsable du traitement, ou qui deviennent nécessaires compte tenu du temps écoulé depuis le traitement initial.

(70 *bis*) Dans de tels cas, une analyse d'impact relative à la protection des données devrait être réalisée par le responsable du traitement (…), préalablement au traitement, en vue d'évaluer la probabilité et la gravité particulières de ce risque élevé, compte tenu de la nature, de la portée, *du contexte et* des finalités du traitement et des sources du risque, et devrait porter notamment sur les dispositions, garanties et mécanismes envisagés pour atténuer ce risque et assurer la protection des données à caractère personnel et pour démontrer que le présent règlement est respecté.

(71) Cela devrait s'appliquer en particulier aux opérations de traitement à grande échelle (...), qui servent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational pouvant affecter un nombre important de personnes concernées et qui sont susceptibles de comporter un risque élevé, par exemple, en raison de leur caractère sensible, lorsque, compte tenu de l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle ainsi qu'à d'autres opérations de traitement qui (...) entraînent un risque élevé pour les droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations, il est plus difficile pour ces dernières d'exercer leurs droits. Une analyse d'impact relative à la protection des données devrait également être effectuée dans les cas où des données sont traitées en vue d'arrêter des décisions relatives à certaines personnes à la suite d'une évaluation systématique et à grande échelle des aspects personnels propres à une personne physique sur la base du profilage desdites données ou à la suite du traitement de catégories particulières de données à caractère personnel, de données biométriques ou de données se rapportant à des condamnations ou des infractions pénales, ou encore à des mesures de sûreté connexes. Une analyse d'impact relative à la protection des données est en outre requise aux fins de la surveillance à grande échelle des zones accessibles au public, en particulier lorsque des dispositifs opto-électroniques sont utilisés, ou pour toute autre opération pour laquelle l'autorité de contrôle compétente considère que le traitement est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes concernées, en particulier parce qu'elles empêchent ces dernières d'exercer un droit ou de bénéficier d'un service ou d'un contrat, ou parce qu'elles sont effectuées systématiquement à grande échelle. *Le traitement (...) de données à caractère personnel, indépendamment de leur volume ou de leur nature, ne devrait pas être considéré comme étant à grand échelle, si le traitement de ces données est protégé par le secret professionnel (...), comme dans le cas du traitement des données à caractère personnel de patients ou clients par un médecin individuel, un professionnel de la santé, un hôpital ou un avocat. Dans de tels cas, une analyse d'impact relative à la protection des données ne devrait pas être obligatoire.*

(72) Il existe des cas dans lesquels il pourrait être judicieux et économique d'élargir l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée.

(73) Une autorité ou un organisme publics peuvent réaliser une analyse d'impact relative à la protection des données si celle-ci n'a pas déjà été faite au moment de l'adoption de la loi nationale régissant la mission de l'autorité ou de l'organisme publics concernés ainsi que l'opération ou l'ensemble d'opérations de traitement en question.

(74) Lorsqu'il ressort d'une analyse d'impact relative à la protection des données que, malgré les garanties, les mesures de sécurité et les mécanismes envisagés pour atténuer le risque, le traitement comporterait un risque élevé pour les droits et les libertés des personnes physiques (...) et que le responsables du traitement est d'avis que le risque ne peut être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il y a lieu de consulter l'autorité de contrôle avant le début des opérations de traitement. Certains types de traitements de données, notamment du fait de leur ampleur et de leur fréquence, sont susceptibles d'entraîner un tel risque (...) élevé et peuvent également (...) causer un dommage ou porter atteinte aux droits et libertés de la personne concernée. L'autorité de contrôle devrait répondre à la demande de consultation dans un délai déterminé. Toutefois, l'absence de réaction de l'autorité de contrôle dans le délai imparti devrait être sans préjudice de toute intervention de sa part dans le cadre des missions et des pouvoirs qui lui sont confiés par le présent règlement, y compris le pouvoir d'interdire des opérations de traitement. Dans le cadre de ce processus de consultation, les résultats d'une analyse d'impact relative à la protection des données réalisée en ce qui concerne le traitement visé à l'article 33 peuvent être soumis à l'autorité de contrôle, notamment pour ce qui est des mesures envisagées pour atténuer le risque pesant sur les droits et libertés des personnes physiques.

(74 *bis*) Le sous-traitant devrait aider le responsable du traitement, s'il y a lieu et sur demande, à assurer le respect des obligations découlant des analyses d'impact relatives à la protection des données et de la consultation préalable de l'autorité de contrôle.

(74 *ter*) L'autorité de contrôle devrait également être consultée au stade de la préparation d'une mesure législative ou réglementaire qui prévoit le traitement de données à caractère personnel (...), afin d'assurer que le traitement envisagé est conforme au présent règlement et, en particulier, d'atténuer le risque qu'il comporte pour la personne concernée.

(75) Lorsque le traitement est réalisé dans le secteur public ou lorsque, dans le secteur privé, il est effectué par une grande entreprise ou par une entreprise, quelle que soit sa taille, dont les activités de base impliquent des opérations de traitement exigeant un suivi régulier et systématique, une personne possédant des connaissances spécialisées de la législation et des pratiques en matière de protection des données peut aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement. Ces délégués à la protection des données, qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et leurs tâches d'une manière indépendante.

(76) Il y a lieu d'encourager les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants à élaborer des codes de conduite, dans le respect du présent règlement, de manière à faciliter sa bonne application, en tenant compte des spécificités des traitements effectués dans certains secteurs et des besoins spécifiques des micro, petites et moyennes entreprises. Ces codes de conduite pourraient en particulier définir les obligations qui incombent aux responsables du traitement et aux sous-traitants, compte tenu du risque auquel le traitement peut exposer les droits et libertés des personnes physiques.

(76 *bis*) Lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations.

(77) Afin de favoriser la transparence et le respect du présent règlement, la création de mécanismes de certification, ainsi que de marques et de labels en matière de protection des données, devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question.

(78) La circulation transfrontière des données à caractère personnel à destination et en provenance de pays tiers et d'organisations internationales est nécessaire au développement de la coopération internationale et du commerce mondial. L'augmentation de ces flux a cependant créé de nouveaux enjeux et de nouvelles préoccupations en ce qui concerne la protection des données à caractère personnel. Or, il importe que, lorsque ces données sont transférées de l'Union vers des responsables du traitement, sous-traitants ou autres destinataires dans des pays tiers ou à des organisations internationales, le niveau de protection des personnes physiques garanti dans l'Union par le présent règlement ne soit pas amoindri, y compris en cas de transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale à des responsables du traitement ou sous-traitants dans le même pays tiers ou dans un pays tiers différent, ou à une autre organisation internationale. En tout état de cause, les transferts vers des pays tiers et à des organisations internationales ne peuvent avoir lieu que dans le plein respect du présent règlement. Un transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions énoncées au chapitre V sont respectées par le responsable du traitement et le sous-traitant.

(79) Le présent règlement ne remet pas en cause les accords internationaux conclus entre l'Union et les pays tiers en vue de réglementer le transfert des données à caractère personnel, y compris les garanties appropriées au bénéfice des personnes concernées. Les États membres peuvent conclure des accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales dans la mesure où ces accords n'affectent pas le présent règlement ou toute autre disposition du droit de l'UE et comportent des garanties visant à protéger les droits des personnes concernées.

(80) La Commission peut décider (...), avec effet dans l'ensemble de l'Union, que certains pays tiers, un territoire ou un secteur déterminé de traitement de données, comme le secteur privé ou un ou plusieurs secteurs économiques spécifiques d'un pays tiers, ou une organisation internationale offrent un niveau de protection des données adéquat, ce qui assurera une sécurité juridique et une uniformité dans toute l'Union au sujet des pays tiers ou des organisations internationales qui sont réputés assurer un tel niveau de protection. Dans ce cas, les transferts de données à caractère personnel vers ces pays peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autorisation spécifique.

(81) Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait, dans son évaluation d'un pays tiers ou d'un territoire ou un secteur déterminé d'un pays tiers, prendre en considération la manière dont ce pays respecte l'État de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, notamment en ce qui concerne la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal. Lors de l'adoption d'une décision d'adéquation relative à un territoire ou à un secteur déterminé d'un pays tiers, il y a lieu de se fonder sur des critères clairs et objectifs, comme les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection, en particulier quand les données sont traitées dans un ou plusieurs secteurs spécifiques. Plus particulièrement, le pays tiers devrait assurer un contrôle effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités européennes de protection des données et les personnes concernées devraient se voir octroyer des droits effectifs et exécutoires ainsi que des possibilités effectives de recours administratif ou juridictionnel.

(81 *bis*) Outre les engagements internationaux pris par le pays tiers ou l'organisation internationale, la Commission devrait également tenir compte des obligations découlant de la participation du pays tiers ou de l'organisation internationale à des systèmes multilatéraux ou régionaux, notamment en matière de protection des données à caractère personnel, ainsi que de la mise en œuvre de ces obligations. *Il y a lieu*, en particulier, *de prendre en considération* l'adhésion du pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel. Aux fins de l'évaluation du niveau de protection assuré par des pays tiers ou des organisations internationales, la Commission devrait consulter le comité européen de la protection des données.

(81 *ter*) La Commission devrait vérifier le fonctionnement des décisions relatives au niveau de protection assuré par un pays tiers, sur un territoire ou dans un secteur déterminé d'un pays tiers, ou par une organisation internationale, y compris les décisions adoptées sur la base de l'article 25, paragraphe 6, ou de l'article 26, paragraphe 4, de la directive 95/46/CE.
Elle devrait évaluer le fonctionnement des dites décisions dans un délai raisonnable et communiquer toute conclusion pertinente au comité au sens du règlement (UE) n° 182/2011 établi en vertu du présent règlement.

(82) La Commission peut (…) constater qu'un pays tiers, un territoire ou un secteur déterminé d'un pays tiers, ou une organisation internationale (…) n'assure plus un niveau adéquat de protection des données. Si tel est le cas, le transfert de données à caractère personnel vers ce pays tiers ou à cette organisation internationale devrait être interdit, à moins que les exigences énoncées aux articles 42 à 44 soient respectées. Il y aurait alors lieu de prendre des dispositions en vue d'une consultation entre la Commission et le pays tiers ou l'organisation internationale. La Commission devrait informer en temps utile le pays tiers ou l'organisation internationale des motifs de sa conclusion et engager des consultations en vue de remédier à la situation.

(83) En l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant devrait prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. Ces garanties peuvent consister à recourir à des règles d'entreprise contraignantes, des clauses types de protection des données adoptées par la Commission, des clauses types de protection des données adoptées par une autorité de contrôle ou des clauses contractuelles ad hoc autorisées par celle-ci, ou d'autres mesures adaptées et proportionnées qui se justifient au regard des circonstances qui entourent une opération ou une série d'opérations de transfert de données, et dans les cas autorisés par une autorité de contrôle. Ces garanties devraient assurer le respect des exigences en matière de protection des données et des droits des personnes concernées, et notamment du droit de recours administratif ou juridictionnel effectif. Elles devraient porter, en particulier, sur le respect des principes généraux concernant le traitement des données à caractère personnel, l'existence de droits exécutoires de la personne concernée et de recours juridictionnels effectifs, ainsi que sur le respect des principes de la protection des données dès la conception et de la protection des données par défaut. Des transferts peuvent également être effectués par des autorités ou organismes publics avec des autorités ou organismes publics dans des pays tiers ou avec des organisations internationales exerçant des tâches ou fonctions correspondantes, y compris sur la base de dispositions à insérer dans des arrangements administratifs, telles qu'un protocole d'accord. L'autorisation de l'autorité de contrôle compétente devrait être obtenue lorsque ces garanties figurent dans des arrangements administratifs qui ne sont pas juridiquement contraignants.

(84) La possibilité qu'ont les responsables du traitement et les sous-traitants de recourir aux clauses types de protection des données adoptées par la Commission ou par une autorité de contrôle ne devrait pas les empêcher d'inclure ces clauses dans un contrat plus large, y compris dans un contrat entre le sous-traitant et un autre sous-traitant, ni d'y ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses contractuelles types adoptées par la Commission ou par une autorité de contrôle et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

(85) Un groupe de sociétés ou un groupe d'entreprises exerçant une activité économique commune devrait être autorisé à recourir à des règles d'entreprise contraignantes pour ses transferts internationaux de l'Union vers des entités du même groupe, à condition que ces règles d'entreprise incluent des principes essentiels et des droits opposables fournissant des garanties appropriées pour les transferts ou catégories de transferts de données à caractère personnel.

(86) Le présent règlement devrait autoriser les transferts dans certains cas où la personne concernée a donné son consentement explicite, lorsque le transfert est occasionnel dans le cadre d'un contrat ou d'une action en justice, qu'il s'agisse d'une procédure judiciaire, administrative ou extrajudiciaire, ou de procédures devant des organismes de régulation. Des dispositions devraient également être prévues pour autoriser les transferts lorsque des motifs importants d'intérêt général établis par le droit de l'Union ou d'un État membre l'exigent, ou lorsque le transfert est effectué à partir d'un registre établi par la loi et destiné à être consulté par le public ou par des personnes y ayant un intérêt légitime. Dans ce cas, un tel transfert ne devrait pas porter sur la totalité des données ni sur des catégories entières de données contenues dans ce registre, et lorsqu'un registre est destiné à être consulté par des personnes qui y ont un intérêt légitime, le transfert ne devrait pouvoir être effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires.

(87) Ces règles devraient s'appliquer en particulier aux transferts de données qui sont nécessaires pour des motifs importants d'intérêt général, par exemple en cas d'échange international de données (...) entre autorités de la concurrence, administrations fiscales ou douanières, entre autorités de surveillance financière, entre services chargés des questions de sécurité sociale ou relatives à la santé publique, par exemple aux fins de la recherche des personnes ayant été en contact avec des personnes atteintes de maladies contagieuses ou en vue de réduire et/ou d'éliminer le dopage dans le sport (...).Le transfert de données à caractère personnel devrait également être considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel en vue de la sauvegarde des intérêts vitaux, y compris l'intégrité physique ou la vie, de la personne concernée ou d'une autre personne, si la personne concernée se trouve dans l'incapacité de donner son consentement. En l'absence de décision d'adéquation, le droit de l'Union ou la législation nationale peut, pour des motifs importants d'intérêt général, fixer expressément des limites au transfert de catégories spécifiques de données vers un pays tiers ou à une organisation internationale. Les États membres devraient notifier ces dispositions à la Commission. Tout transfert vers une organisation humanitaire internationale, par exemple une société nationale de la Croix-Rouge (…) ou le CICR, de données à caractère personnel d'une personne concernée qui se trouve dans l'incapacité physique ou juridique de donner son consentement, en vue d'accomplir une mission qui incombe au Mouvement international de la Croix-Rouge et du Croissant-Rouge en application des Conventions de Genève et/ou de contribuer à l'application fidèle du droit humanitaire international applicable dans les conflits armés, pourrait être considéré comme nécessaire pour des motifs importants d'intérêt général ou pour la sauvegarde de l'intérêt vital de la personne concernée.

(88) Les transferts qui ne peuvent être qualifiés de transferts à grande échelle ou fréquents pourraient également être autorisés aux fins de la poursuite des intérêts légitimes du responsable du traitement ou du sous-traitant, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée et si le responsable du traitement ou le sous-traitant a évalué toutes les circonstances entourant le transfert. Le responsable du traitement ou le sous-traitant devrait accorder une attention particulière à la nature des données, à la finalité et à la durée du ou des traitements envisagés ainsi qu'à la situation dans le pays d'origine, dans le pays tiers et dans le pays de destination finale, et aux garanties appropriées offertes pour protéger les droits fondamentaux et les libertés fondamentales des personnes physiques au regard du traitement des données à caractère personnel les concernant. Pour les traitements à des fins historiques, statistiques et scientifiques, il y aurait lieu de prendre en considération les attentes légitimes de la société en matière de progrès des connaissances. Pour évaluer si un transfert est à grande échelle ou fréquent, il convient de prendre en considération le volume de données à caractère personnel et le nombre de personnes concernées, et d'examiner si le transfert s'effectue sur une base occasionnelle ou régulière.

(89) En tout état de cause, lorsque la Commission ne s'est pas prononcée sur le caractère adéquat de la protection des données dans un pays tiers, le responsable du traitement ou le sous-traitant devrait adopter des solutions qui garantissent aux personnes concernées qu'elles continueront de bénéficier des droits fondamentaux et des garanties qui leur sont accordés dans l'Union pour le traitement des données les concernant, une fois que ces données auront été transférées.

(90) Certains pays tiers édictent des lois, des règlements et d'autres instruments législatifs qui visent à régir directement des activités de traitement des données effectuées par des personnes physiques et morales qui relèvent de la compétence des États membres. L'application extraterritoriale de ces lois, règlements et autres instruments législatifs peut être contraire au droit international et faire obstacle à la protection des personnes garantie dans l'Union par le présent règlement. Les transferts ne devraient donc être autorisés que lorsque les conditions fixées par le présent règlement pour les transferts vers les pays tiers sont remplies. Ce peut être le cas, notamment, lorsque la divulgation est nécessaire pour un motif important d'intérêt général reconnu par le droit de l'Union ou par le droit d'un État membre auquel le responsable des données est soumis. (...)

(91) Lorsque des données à caractère personnel franchissent les frontières extérieures de l'Union, elles accroissent le risque que les personnes physiques ne puissent exercer leur droit à la protection des données, notamment pour se protéger de l'utilisation ou de la divulgation illicite de ces informations. De même, les autorités de contrôle peuvent être confrontées à l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités exercées en dehors de leurs frontières. Leurs efforts pour collaborer dans le contexte transfrontière peuvent également être freinés par les pouvoirs insuffisants dont elles disposent en matière de prévention ou de recours, par l'hétérogénéité des régimes juridiques et par des obstacles pratiques tels que le manque de ressources. En conséquence, il est nécessaire de favoriser une coopération plus étroite entre les autorités de contrôle de la protection des données, afin qu'elles puissent échanger des informations et mener des enquêtes avec leurs homologues internationaux. Aux fins d'élaborer des mécanismes de coopération internationale visant à faciliter et à mettre en place une assistance mutuelle internationale pour l'application de la législation relative à la protection des données à caractère personnel, la Commission et les autorités de contrôle devraient échanger des informations et coopérer dans le cadre d'activités liées à l'exercice de leurs compétences avec les autorités compétentes dans les pays tiers, sur une base réciproque et dans le respect des dispositions du présent règlement, et notamment des dispositions du chapitre V.

(92) La création d'autorités de contrôle dans les États membres, habilitées à remplir leurs missions et à exercer leurs compétences en toute indépendance, est un élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Les États membres ont la possibilité de créer plusieurs autorités de contrôle en fonction de leur structure constitutionnelle, organisationnelle et administrative.

(92 *bis*) Le fait que les autorités de contrôle soient indépendantes ne devrait pas signifier qu'elles ne peuvent être soumises à un mécanisme de contrôle ou de suivi de leur gestion financière, ni qu'elles ne peuvent être soumises à un contrôle juridictionnel.

(93) Lorsqu'un État membre crée plusieurs autorités de contrôle, il devrait prévoir, dans sa législation, des dispositifs garantissant la participation effective de ces autorités au mécanisme de contrôle de la cohérence. Il devrait en particulier désigner l'autorité de contrôle qui servira de point de contact unique, permettant une participation efficace de ces autorités au mécanisme, afin d'assurer une coopération rapide et aisée avec les autres autorités de contrôle, le comité européen de la protection des données et la Commission.

(94) Il convient que chaque autorité de contrôle soit dotée de (…) tous les moyens financiers et humains, ainsi que locaux et infrastructures nécessaires à la bonne exécution de ses missions, y compris celles qui sont liées à l'assistance mutuelle et à la coopération avec d'autres autorités de contrôle dans l'ensemble de l'Union. Chaque autorité de contrôle devrait disposer d'un budget annuel propre pouvant faire partie du budget général de l'État ou du budget national.

(95) Les conditions générales applicables au(x) membre(s) de l'autorité de contrôle devraient être fixées par la loi dans chaque État membre et prévoir notamment que ces membres sont nommés par le parlement, et/ou le gouvernement ou chef d'État de cet État membre ou par un organisme indépendant chargé, par la législation de l'État membre, de procéder à la nomination selon une procédure transparente. Afin de garantir l'indépendance de l'autorité de contrôle, le membre ou les membres de celle-ci s'abstiennent de tout acte incompatible avec leurs fonctions et n'exercent, pendant la durée de leur mandat, aucune activité professionnelle incompatible, rémunérée ou non. (…).

(95 *bis*) Chaque autorité de contrôle devrait être compétente sur le territoire de l'État membre dont elle relève pour exercer les pouvoirs et accomplir les missions dont elle est investie conformément au présent règlement. Sont concernés en particulier le traitement dans le cadre d'activités menées par un établissement du responsable du traitement ou du sous-traitant sur le territoire de l'État membre dont elle relève, le traitement de données à caractère personnel effectué par des autorités publiques ou des organismes privés agissant dans l'intérêt public, le traitement affectant des personnes concernées sur le territoire de l'État membre dont elle relève, ou encore le traitement effectué par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union européenne lorsqu'il vise des personnes concernées établies sur le territoire de l'État membre dont elle relève. Il s'agit notamment de traiter les réclamations introduites par les personnes concernées, d'effectuer des enquêtes sur l'application du règlement et de sensibiliser le public sur les risques, les règles, les garanties et les droits relatifs au traitement des données à caractère personnel.

(96) Il appartient aux autorités de contrôle de surveiller l'application des dispositions du présent règlement et de contribuer à ce que cette application soit cohérente dans l'ensemble de l'Union, afin de protéger les personnes physiques à l'égard du traitement de leurs données à caractère personnel et de faciliter la libre circulation de ces données au sein du marché intérieur. À cette fin, le présent règlement devrait imposer aux autorités de contrôle de coopérer entre elles et avec la Commission et leur permettre de le faire sans qu'un accord doive être conclu entre les États membres sur la fourniture d'une assistance mutuelle ou sur une telle coopération.

(97) Lorsque le traitement des données à caractère personnel se déroule dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant dans l'Union et que ce responsable du traitement ou ce sous-traitant est établi dans plusieurs États membres, ou que le traitement se déroulant dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant dans l'Union affecte ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres, l'autorité de contrôle dont relève l'établissement principal du responsable du traitement ou du sous-traitant ou l'établissement unique du responsable du traitement ou du sous-traitant devrait faire office d'autorité chef de file. Elle devrait coopérer avec les autres autorités concernées dans la mesure où le responsable du traitement ou le sous-traitant a un établissement sur le territoire de l'État membre dont elles relèvent, dans la mesure où les personnes concernées résidant sur le territoire dont elles relèvent sont sensiblement affectées ou encore dans la mesure où une réclamation leur a été adressée. En outre, lorsqu'une personne concernée ne résidant pas dans cet État membre a introduit une réclamation, l'autorité de contrôle auprès de laquelle celle-ci a été introduite devrait également constituer une autorité de contrôle concernée. Dans le cadre de ses missions liées à la publication de lignes directrices sur toute question portant sur l'application du présent règlement, le comité européen de la protection des données peut diffuser des lignes directrices portant, en particulier, sur les critères à prendre en compte afin de vérifier si le traitement en question affecte sensiblement des personnes concernées dans plusieurs États membres et sur ce qui constitue une objection pertinente et motivée.

(97 *bis*) L'autorité chef de file devrait être compétente pour adopter des décisions contraignantes concernant les mesures visant à mettre en œuvre les pouvoirs qui lui sont conférés conformément aux dispositions du présent règlement. En sa qualité d'autorité chef de file, l'autorité de contrôle devrait associer de près les autorités de contrôle concernées au processus décisionnel et assurer une coordination étroite dans ce cadre. Lorsque qu'il est décidé de rejeter, en tout ou en partie, la réclamation introduite par la personne concernée, cette décision devrait être adoptée par l'autorité de contrôle auprès de laquelle la réclamation a été introduite.

(97 *ter*) La décision devrait être adoptée conjointement par l'autorité de contrôle chef de file et les autorités de contrôle concernées, être adressée à l'établissement principal ou unique du responsable du traitement ou du sous-traitant et être contraignante pour le responsable du traitement et le sous-traitant. Le responsable du traitement ou le sous-traitant devraient prendre les mesures nécessaires pour garantir le respect du présent règlement et l'application de la décision notifiée par l'autorité de contrôle chef de file à l'établissement principal du responsable du traitement ou du sous-traitant en ce qui concerne les activités de traitement dans l'Union.

(97 *quater*) Chaque autorité de contrôle qui ne fait (...) pas office de chef de file devrait être compétente pour traiter les cas de portée locale, en d'autres termes, les cas où le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres mais où l'objet du traitement spécifique ne se rapporte qu'à un traitement effectué dans un seul État membre et ne portant que sur des personnes concernées de ce seul État membre, par exemple lorsqu'il s'agit de traiter des données relatives à des employés dans le contexte professionnel propre à un État membre. Dans ces cas, l'autorité de contrôle informe sans tarder l'autorité de contrôle chef de file de la question. Après avoir été informée, l'autorité de contrôle chef de file devrait décider si elle traitera le cas dans le cadre du mécanisme de guichet unique ou si l'autorité de contrôle qui l'a informée devrait le traiter au niveau local. Lorsqu'elle décide si elle traitera le cas, l'autorité de contrôle chef de file devrait tenir compte du point de savoir s'il existe un établissement du responsable du traitement ou du sous-traitant dans l'État membre de l'autorité de contrôle qui l'a informée, afin d'assurer l'application efficace d'une décision à l'égard du responsable du traitement ou du sous-traitant. Si l'autorité de contrôle chef de file décide de traiter le cas, l'autorité de contrôle qui l'a informée devrait avoir la possibilité de soumettre un projet de décision, dont l'autorité de contrôle chef de file devrait tenir de le plus grand compte lorsqu'elle élabore son projet de décision dans le cadre du mécanisme de guiche unique.

(98) Les règles relatives à l'autorité de contrôle chef de file et au mécanisme de guichet unique ne devraient pas être applicables lorsque le traitement est effectué par des autorités publiques ou des organismes privés agissant dans l'intérêt public. Dans ce cas, la seule autorité de contrôle compétente pour exercer les pouvoirs qui lui sont conférés en vertu du présent règlement devrait être l'autorité de contrôle de l'État membre dans lequel l'autorité publique ou l'organisme privé sont établis.

(99) (...)

(100) Afin d'assurer la cohérence du contrôle et de l'application du présent règlement dans l'ensemble de l'Union, les autorités de contrôle devraient avoir, dans chaque État membre, les mêmes missions et les mêmes pouvoirs effectifs, dont celui d'enquêter, d'adopter des mesures correctrices et des sanctions, de même que celui d'autoriser et de délibérer, en particulier en cas de réclamation introduite par des personnes physiques, et, sans préjudice des pouvoirs des autorités chargées des poursuites en droit national, le pouvoir de porter les infractions au présent règlement à l'attention des autorités judiciaires et/ou d'ester en justice. Ces pouvoirs devraient également inclure celui d'interdire les traitements au sujet desquels l'autorité est consultée. Les États membres peuvent prévoir que d'autres missions sont spécifiquement liées à la protection des données à caractère personnel en application du présent règlement. Les pouvoirs des autorités de contrôle (...) devraient être exercés en conformité avec les garanties procédurales appropriées prévues par le droit de l'Union et la législation nationale, d'une manière impartiale et équitable et dans un délai raisonnable. Cela signifie que toute mesure devrait être appropriée, nécessaire et proportionnée en vue de garantir le respect du présent règlement, compte tenu des circonstances de l'espèce, respecter le droit de chacun à être entendu avant que soit prise toute mesure individuelle susceptible de l'affecter défavorablement et éviter les coûts superflus ainsi que les désagréments excessifs pour les personnes concernées. Les pouvoirs d'enquête en ce qui concerne l'accès aux installations devraient être exercés dans le respect des exigences spécifiques du droit procédural national, par exemple de l'obligation d'obtenir une autorisation judiciaire préalable.

Toute mesure juridiquement contraignante prise par l'autorité de contrôle devrait être présentée par écrit, claire et dénuée d'ambiguïté, indiquer quelle autorité de contrôle a pris la mesure et à quelle date, porter la signature du chef ou d'un membre de l'autorité de contrôle qu'il a autorisée, exposer les motifs qui sous-tendent la mesure et mentionner le droit à un recours effectif, sans préjudice des exigences supplémentaires prévues par le droit procédural national, sans préjudice des exigences supplémentaires prévues par le droit procédural national. Si une telle décision juridiquement contraignante est adoptée, elle peut donner lieu à un contrôle juridictionnel dans l'État membre de l'autorité de contrôle qui l'a adoptée.

(101) (…)

(101 *bis*) Lorsque l'autorité de contrôle auprès de laquelle la réclamation a été introduite n'est pas l'autorité de contrôle chef de file, l'autorité de contrôle chef de file devrait coopérer étroitement avec l'autorité de contrôle auprès de laquelle la réclamation a été introduite conformément aux dispositions relatives à la coopération et à la cohérence prévues par le présent règlement. Dans de tels cas, l'autorité de contrôle chef de file devrait, lorsqu'elle adopte des mesures visant à produire des effets juridiques, y compris des mesures visant à infliger des amendes administratives, tenir le plus grand compte de l'avis de l'autorité de contrôle auprès de laquelle la réclamation a été introduite, laquelle devrait rester compétente pour effectuer toute enquête sur le territoire de l'État membre dont elle relève, en liaison avec l'autorité de contrôle compétente.

(101 *ter*) L'autorité de contrôle qui est saisie d'une réclamation, qui constate des situations susceptibles de constituer des infractions au présent règlement ou qui est informée d'une autre manière de telles situations, devrait rechercher un règlement amiable et, en cas d'échec, exercer l'ensemble de ses pouvoirs dans les cas où, même si c'est une autre autorité de contrôle qui devrait être chef de file pour les activités de traitement du responsable du traitement ou du sous-traitant, l'objet concret d'une réclamation ou l'infraction éventuelle ne concerne que les activités de traitement du responsable du traitement ou du sous-traitant dans l'État membre dans lequel la réclamation a été introduite ou dans lequel l'infraction éventuelle a été constatée et que l'objet n'affecte pas sensiblement ou n'affectera probablement pas sensiblement des personnes concernées dans d'autres États membres. Devraient être concernés les traitements spécifiques qui sont effectués sur le territoire de l'État membre dont relève l'autorité de contrôle ou qui portent sur des personnes concernées se trouvant sur le territoire de cet État membre, les traitements effectués dans le cadre d'une offre de biens ou de services visant spécifiquement des personnes concernées se trouvant sur le territoire de l'État membre dont relève l'autorité de contrôle ou encore les traitements qui doivent être évalués à l'aune des obligations légales applicables prévues par le droit national.

(102) Les activités de sensibilisation organisées par les autorités de contrôle à l'intention du public devraient comprendre des mesures spécifiques destinées aux responsables du traitement et aux sous-traitants, y compris les microentreprises et les petites et moyennes entreprises, et aux particuliers, notamment dans le contexte éducatif.

(103) Les autorités de contrôle devraient s'entraider et se prêter mutuellement assistance dans l'exercice de leurs missions afin d'assurer une application cohérente du présent règlement dans le marché intérieur. Lorsqu'une autorité de contrôle qui a fait appel à l'assistance mutuelle n'a pas reçu de réponse de l'autorité de contrôle sollicitée dans un délai d'un mois à compter de la réception de la demande, adopte une mesure provisoire, cette mesure provisoire devrait être dûment motivée et uniquement de nature temporaire.

(104) Chaque autorité de contrôle devrait avoir le droit de participer à des opérations conjointes entre autorités de contrôle. L'autorité de contrôle requise devrait être tenue de répondre à la demande dans un délai déterminé.

(105) Afin de garantir l'application cohérente du présent règlement dans l'ensemble de l'Union, il y a lieu d'instaurer un mécanisme de contrôle de la cohérence encadrant la coopération entre les autorités de contrôle (...). Ce mécanisme devrait notamment s'appliquer lorsqu'une autorité de contrôle a l'intention d'adopter une mesure destinée à produire des effets juridiques à l'égard de traitements qui affectent sensiblement un nombre important de personnes concernées dans plusieurs États membres (…). Il devrait également s'appliquer lorsqu'une autorité de contrôle concernée ou la Commission demande que ce type de question soit traitée dans le cadre du mécanisme de contrôle de la cohérence. Ce mécanisme devrait s'appliquer sans préjudice des éventuelles mesures que la Commission pourrait prendre dans l'exercice des compétences que lui confèrent les traités.

(106) En application du mécanisme de contrôle de la cohérence, le comité européen de la protection des données devrait émettre un avis, dans un délai déterminé, si une majorité (…) de ses membres le décide ou s'il est saisi d'une demande en ce sens par une autorité de contrôle concernée ou par la Commission. Le comité européen de la protection des données devrait également être habilité à adopter des décisions juridiquement contraignantes en cas de différend entre autorités de contrôle. À cet effet, il devrait prendre, en principe à la majorité des deux tiers de ses membres, des décisions juridiquement contraignantes dans des cas clairement définis, en cas de divergence de vues entre autorités de contrôle, notamment dans le cadre du mécanisme de coopération entre l'autorité de contrôle chef de file et les autorités de contrôle concernées, sur le fond de l'affaire et en particulier sur la question de savoir s'il y a infraction ou pas.

(107) (...)

(108) Il peut être nécessaire d'agir de toute urgence pour protéger les droits et les libertés des personnes concernées, en particulier lorsque l'exercice du droit d'une personne concernée risque d'être considérablement entravé. En conséquence, lorsqu'elle applique le mécanisme de contrôle de la cohérence, l'autorité de contrôle devrait pouvoir adopter des mesures provisoires d'une durée déterminée.

(109) La mise en œuvre de ce mécanisme devrait conditionner la légalité d'une mesure destinée à produire des effets juridiques prise par une autorité de contrôle dans les cas où cette mise en œuvre est obligatoire. Dans d'autres cas présentant une dimension transfrontière, le mécanisme de coopération entre l'autorité de contrôle chef de file et les autorités de contrôle concernées devrait être appliqué, et l'assistance mutuelle ainsi que des opérations conjointes pourraient être mises en œuvre par les autorités de contrôle concernées, sur une base bilatérale ou multilatérale, sans faire jouer le mécanisme de contrôle de la cohérence.

(110) Afin de favoriser l'application cohérente du présent règlement, le comité européen de la protection des données devrait être institué en tant qu'organe indépendant de l'Union. Pour pouvoir atteindre ses objectifs, le comité devrait être doté de la personnalité juridique. Il devrait être représenté par son président. Il devrait remplacer le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par la directive 95/46/CE. Il devrait se composer d'un directeur d'une autorité de contrôle de chaque État membre ou de son représentant (...). La Commission et le contrôleur européen de la protection des données devraient participer à ses activités sans bénéficier du droit de vote. Le comité européen de la protection des données devrait contribuer à l'application cohérente du présent règlement dans toute l'Union, notamment en conseillant la Commission, en particulier en ce qui concerne le niveau de protection dans les pays tiers ou les organisations internationales, et en favorisant la coopération des autorités de contrôle dans l'ensemble de l'Union. Il devrait remplir ses missions en toute indépendance.

(110 *bis*) Le comité européen de la protection des données devrait être assisté par un secrétariat assuré par le secrétariat du contrôleur européen de la protection des données. Pour s'acquitter de ses tâches, le personnel du secrétariat du contrôleur européen de la protection des données chargé de missions que le présent règlement confie au comité européen de la protection des données ne devrait recevoir ses instructions que du président du comité européen de la protection des données et devrait être placé sous l'autorité de celui-ci. La séparation organisationnelle du personnel devrait concerner tous les services nécessaires au fonctionnement indépendant du comité européen de la protection des données.

111) Toute personne concernée devrait avoir le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre où elle a sa résidence habituelle, et disposer d'un droit à un recours juridictionnel effectif conformément à l'article 47 de la Charte des droits fondamentaux de l'Union européenne si elle estime que les droits que lui confère le présent règlement ne sont pas respectés ou si l'autorité de contrôle ne donne pas suite à une réclamation, si elle la refuse ou la rejette, en tout ou en partie, ou si elle n'agit pas alors qu'une action est nécessaire pour protéger les droits de la personne concernée. L'enquête faisant suite à une réclamation devrait être menée, sous réserve d'un contrôle juridictionnel, dans la mesure appropriée requise par l'affaire. L'autorité de contrôle devrait informer la personne concernée de l'état d'avancement et du résultat de la réclamation dans un délai raisonnable. Si l'affaire requiert un complément d'enquête ou une coordination avec une autre autorité de contrôle, des informations intermédiaires devraient être fournies à la personne concernée. Afin de faciliter l'introduction des réclamations, chaque autorité de contrôle devrait prendre des mesures telles que la fourniture d'un formulaire de réclamation qui peut être rempli également par voie électronique, sans que d'autres moyens de communication soient exclus.

(112) Lorsqu'une personne concernée estime que les droits que lui confère le présent règlement ne sont pas respectés, elle devrait avoir le droit de mandater un organisme, une organisation ou une association qui œuvrent à la protection des droits et intérêts des personnes concernées dans le domaine de la protection des données et qui sont constitués conformément au droit national pour qu'ils introduisent une réclamation en son nom auprès d'une autorité de contrôle ou pour qu'ils exercent le droit à un recours juridictionnel au nom de personnes concernées. Les États membres peuvent disposer que cet organisme, cette organisation ou cette association devraient avoir le droit d'introduire une réclamation dans l'État membre en question, indépendamment de tout mandat d'une personne concernée, et/ou disposer d'un droit à un recours juridictionnel effectif s'ils ont des raisons de considérer que (...) les droits d'une personne concernée n'ont pas été respectés parce que le traitement des données à caractère personnel n'a pas eu lieu en conformité avec le présent règlement. Cet organisme, cette organisation ou cette association ne peut pas être autorisé à réclamer une indemnisation pour le compte d'une personne concernée.

(113) Toute personne physique ou morale a le droit de former un recours en annulation des décisions du comité européen de la protection des données devant la Cour de justice de l'Union européenne (ci-après désignée "la Cour de justice") selon les conditions prévues à l'article 263 du TFUE. En tant que destinataires de telles décisions, les autorités de contrôle concernées qui souhaitent former un recours à leur encontre doivent le faire dans un délai de deux mois à compter de la notification qui leur en a été faite, conformément à l'article 263 du TFUE. Lorsque des décisions du comité européen de la protection des données concernent directement et individuellement un responsable du traitement, un sous-traitant ou la personne à l'origine de la réclamation, ils peuvent former un recours en annulation de ces décisions dans un délai de deux mois à compter de leur publication sur le site web du comité européen de la protection des données, conformément à l'article 263 du TFUE. Sans préjudice de ce droit prévu à l'article 263 du TFUE, toute personne physique ou morale devrait disposer d'un recours juridictionnel effectif, devant la juridiction nationale compétente, contre une décision d'une autorité de contrôle qui produit des effets juridiques à son égard. Une telle décision concerne en particulier l'exercice, par l'autorité de contrôle, de pouvoirs d'enquête, de pouvoirs correctifs et de pouvoirs d'autorisation ou la révocation ou le rejet de réclamations. Toutefois, ce droit ne concerne pas d'autres mesures des autorités de contrôle qui ne sont pas juridiquement contraignantes, telles que les avis émis ou les conseils fournis par une autorité de contrôle. Les actions contre une autorité de contrôle devraient être intentées devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie et être menées conformément au droit procédural national de l'État membre en question.
Ces juridictions devraient disposer d'une pleine compétence, et notamment de celle d'examiner tous les éléments de fait et de droit relatifs au litige dont elles sont saisies.
Lorsqu'une réclamation a été rejetée ou révoquée par une autorité de contrôle, la personne à l'origine de la réclamation peut intenter une action devant les juridictions de ce même État membre. Dans le cadre des recours juridictionnels relatifs à l'application du présent règlement, les juridictions nationales qui estiment qu'une décision sur ce point est nécessaire pour rendre leur jugement peuvent ou, dans le cas prévu à l'article 267 du TFUE, doivent demander à la Cour de justice de statuer à titre préjudiciel sur l'interprétation du droit de l'Union, y compris le présent règlement.

En outre, lorsqu'une décision d'une autorité de contrôle mettant en œuvre une décision du comité européen de la protection des données fait l'objet d'un recours devant une juridiction nationale et que la validité de la décision du comité européen de la protection des données est en question, ladite juridiction nationale n'est pas habilitée à déclarer invalide la décision du comité européen de la protection des données et doit, dans tous les cas où elle considère qu'une décision est invalide, soumettre la question de la validité à la Cour de justice, conformément à l'article 267 du TFUE tel qu'il a été interprété par la Cour de justice dans l'affaire Foto-Frost[1]. Toutefois, une juridiction nationale peut ne pas soumettre une question relative à la validité d'une décision du comité européen de la protection des données à la demande d'une personne physique ou morale qui a eu la possibilité de former un recours en annulation de cette décision, en particulier si elle était concernée directement et individuellement par ladite décision, et ne l'a pas fait dans le délai prévu à l'article 263 du TFUE.

(113 *bis*) Lorsqu'une juridiction saisie d'un recours contre une décision prise par une autorité de contrôle a des raisons de croire que d'autres recours concernant le même traitement, portant par exemple sur le même objet, des activités du même responsable du traitement ou du même sous-traitant, ou encore la même cause, ont été introduits devant une juridiction compétente d'un autre État membre, il conviendrait qu'elle entre en contact avec cette autre juridiction afin de confirmer l'existence de tels recours connexes. Si des recours connexes sont pendants devant une juridiction d'un autre État membre, toute juridiction autre que celle qui a été saisie en premier peut surseoir à statuer ou peut, sur demande de l'une des parties, se dessaisir au profit de la première juridiction saisie si celle-ci est compétente pour connaître de l'action concernée et que la législation applicable permet de regrouper de tels recours connexes. Sont réputés connexes les recours qui sont à ce point étroitement liés qu'il y a intérêt à les instruire et à les juger en même temps afin d'éviter que ne soient rendues des décisions inconciliables, issues de procédures séparées.

(114) (...)

(115) (...)

---

[1] Affaire C-314/85

(116) En ce qui concerne les recours à l'encontre d'un responsable du traitement ou d'un sous-traitant, le demandeur devrait pouvoir choisir d'intenter l'action devant les juridictions des États membres dans lesquels le responsable du traitement ou le sous-traitant a un établissement ou dans l'État membre dans lequel la personne concernée réside, sauf si le responsable du traitement est une autorité publique agissant dans l'exercice de la puissance publique.

(117) (…)

(118) Tout dommage qu'une personne pourrait subir du fait d'un traitement non conforme au présent règlement devrait être réparé par le responsable du traitement ou le sous-traitant, qui devrait cependant être exonéré de sa responsabilité s'il prouve que le dommage ne lui est en aucune manière imputable (…). La notion de dommage devrait être interprétée au sens large, à la lumière de la jurisprudence de la Cour de justice de l'Union européenne, de façon à tenir pleinement compte des objectifs du présent règlement. Cela est sans préjudice de toute action en dommages-intérêts fondée sur une infraction à d'autres règles du droit de l'Union ou d'un État membre. (...)
Lorsqu'il est fait référence à un traitement non conforme au présent règlement, cela concerne aussi un traitement non conforme aux actes délégués et d'exécution adoptés conformément au présent règlement et à la législation nationale précisant les règles de mise en œuvre du présent règlement.

Les personnes concernées devraient recevoir une indemnisation complète et effective pour le dommage subi. Lorsque des responsables du traitement ou des sous-traitants participent à un même traitement, chaque responsable du traitement ou chaque sous-traitant devrait être tenu responsable pour l'entièreté du dommage. Toutefois, s'ils peuvent être regroupés dans le cadre d'un même recours juridictionnel, conformément au droit national, l'indemnisation peut être répartie en fonction de la responsabilité de chaque responsable du traitement ou de chaque sous-traitant pour le dommage causé par le traitement, à condition que la personne concernée qui a subi le dommage soit entièrement et effectivement indemnisée. Tout responsable du traitement ou tout sous-traitant qui (…) a versé une indemnisation complète peut par la suite introduire un recours contre d'autres responsables du traitement ou sous-traitants ayant participé au même traitement.

(118 *bis*) Lorsque le présent règlement prévoit des règles juridictionnelles spécifiques, notamment en ce qui concerne les recours juridictionnels, y compris ceux qui visent à obtenir une indemnisation, à l'encontre d'un responsable du traitement ou d'un sous-traitant, les règles juridictionnelles générales, telles que celles prévues dans le règlement (UE) n° 1215/2012, devraient être sans préjudice de l'application de telles règles juridictionnelles spécifiques.

(118 *ter*) Afin de renforcer le contrôle de l'application des dispositions du présent règlement, des sanctions et des amendes administratives peuvent être infligées pour toute violation du règlement, en plus ou à la place des mesures appropriées imposées par l'autorité de contrôle conformément au présent règlement. En cas d'infraction mineure ou si l'amende susceptible d'être infligée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende. Il conviendrait toutefois de tenir dûment compte de la nature, de la gravité et de la durée de l'infraction, du caractère intentionnel de l'infraction et des mesures prises pour limiter le dommage subi, du degré de responsabilité ou *de toute infraction* pertinente *commise précédemment*, de la manière dont l'infraction a été portée à la connaissance de l'autorité de contrôle, du respect des mesures ordonnées contre le responsable du traitement ou le sous-traitant, de l'adhésion à un code de conduite et de tout autre facteur aggravant ou atténuant. L'application de sanctions et d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la charte des droits fondamentaux, y compris le droit à une protection judiciaire effective et à une procédure régulière. Lorsque le droit national d'un État membre ne prévoit pas d'amende administrative, cet État membre peut ne pas infliger de telles amendes pour les infractions au présent règlement qui relèvent déjà du droit pénal en droit national et veiller à ce que ces sanctions pénales soient effectives, proportionnées et dissuasives, compte tenu du niveau des amendes administratives prévues dans le présent règlement.

(119) Les États membres peuvent fixer les règles relatives aux sanctions pénales infligées pour les violations du présent règlement, y compris les violations de dispositions nationales adoptées en application et dans les limites du présent règlement. Ces sanctions pénales peuvent aussi permettre la saisie des profits réalisés en infraction au présent règlement. Toutefois, l'application de sanctions pénales en cas de violation de ces dispositions nationales et de sanctions administratives ne devrait pas entraîner la violation du principe "*ne bis in idem*" tel qu'il a été interprété par la Cour de justice.

(120) Afin de renforcer et d'harmoniser les amendes administratives applicables en cas de violation du présent règlement, chaque autorité de contrôle devrait avoir le pouvoir d'infliger des amendes administratives. Le présent règlement devrait définir les infractions, le montant maximal et les critères d'établissement des amendes administratives dont elles sont passibles, qui devraient être fixées par l'autorité de contrôle compétente dans chaque cas, eu égard à toutes les circonstances pertinentes de la situation spécifique et compte dûment tenu, notamment, de la nature, de la gravité et de la durée de l'infraction et de ses conséquences, ainsi que des mesures prises pour garantir le respect des obligations imposées au titre du règlement et pour prévenir ou atténuer les conséquences de la violation. Lorsque les amendes sont imposées à des personnes qui ne sont pas une entreprise commerciale, l'autorité de contrôle devrait tenir compte du niveau général des revenus dans l'État membre lorsqu'elle examine quel serait le montant approprié de l'amende. Il pourrait en outre être recouru au mécanisme de contrôle de la cohérence pour favoriser une application cohérente des amendes administratives. Il devrait appartenir aux États membres de déterminer si les autorités publiques devraient être soumises à des amendes administratives, et dans quelle mesure. L'application d'une amende administrative ou le fait de donner un avertissement ne portent pas atteinte à l'exercice d'autres pouvoirs des autorités de contrôle ou à l'application d'autres sanctions en vertu du règlement.

(120 *bis*) Lorsque le présent règlement n'harmonise pas les amendes administratives ou, au besoin, dans d'autres circonstances, par exemple en cas d'infraction grave au présent règlement, les États membres devraient mettre en œuvre un système qui prévoit des sanctions effectives, proportionnées et dissuasives. La nature de ces sanctions (sanctions pénales ou amendes administratives) devrait être déterminée par la législation nationale.

(121) La législation des États membres devrait concilier les règles régissant la liberté d'expression et d'information, y compris l'expression journalistique, universitaire, artistique ou littéraire, et le droit à la protection des données à caractère personnel au titre du présent règlement. Dans le cadre du traitement de données à caractère personnel à des fins de journalisme ou à des fins d'expression universitaire, artistique ou littéraire, il y a lieu de prévoir des dérogations ou des exemptions à certaines dispositions du présent règlement si cela est nécessaire pour concilier le droit à la protection de ces données et le droit à la liberté d'expression et d'information, garanti par l'article 11 de la charte des droits fondamentaux de l'Union européenne.
Tel devrait notamment être le cas des traitements de données à caractère personnel dans le domaine de l'audiovisuel et dans les documents d'archives et bibliothèques de journaux.
En conséquence, les États membres devraient adopter des mesures législatives qui prévoient les exemptions et dérogations nécessaires pour assurer l'équilibre avec ces droits fondamentaux. Les États membres devraient adopter de telles exemptions et dérogations en ce qui concerne les principes généraux, les droits de la personne concernée, le responsable des données et le sous-traitant, le transfert de données vers des pays tiers ou à des organisations internationales, les autorités de contrôle indépendantes, et la coopération et la cohérence.
Dans le cas où ces exemptions ou dérogations diffèrent d'un État membre à l'autre, la législation nationale de l'État membre dont relève le responsable du traitement devrait s'appliquer. Pour tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique, il y a lieu de retenir une interprétation large des notions liées à cette liberté, comme le journalisme. (...)

(121 *bis*) *Le présent règlement permet de prendre en compte, dans l'application de ses dispositions, le principe de l'accès du public aux documents officiels. L'accès du public au documents officiels peut être considéré comme un intérêt public. Les données à caractère personnel figurant dans des documents détenus par une autorité publique ou un organisme public devraient pouvoir être divulguées par ladite autorité ou ledit organisme si cette divulgation est prévue par le droit de l'Union ou le droit de l'État membre dont relève l'autorité ou l'organisme. Ces législations devraient concilier l'accès du public aux documents officiels et la réutilisation des informations du secteur public, d'une part, et le droit à la protection des données à caractère personnel, d'autre part, et peuvent donc prévoir les dérogations nécessaires aux règles du présent règlement. Dans ce contexte, il convient d'entendre par "autorités et organismes publics" toutes les autorités ou les autres organismes relevant de la législation de l'État membre en matière d'accès du public aux documents. La directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public laisse intact et n'affecte en rien le niveau de protection des personnes à l'égard du traitement des données à caractère personnel garanti par les dispositions du droit de l'Union et du droit national et, en particulier, ne modifie en rien les droits et obligations prévus dans le présent règlement. En particulier, ladite directive ne devrait pas s'appliquer aux documents dont l'accès est exclu ou limité en application de règles d'accès pour des motifs de protection des données à caractère personnel, et aux parties de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été définie par la loi comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel.*

(122) (…).

(123) (…).

(124) La législation nationale ou des conventions collectives (y compris des "accords d'entreprise") *peuvent prévoir des règles spécifiques pour le traitement des données à caractère personnel des salariés en matière d'emploi, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.*

(125) Outre les principes généraux et les règles spécifiques prévus dans le présent règlement concernant en particulier les conditions de licéité du traitement, le traitement des données à caractère personnel à des fins historiques (...), statistiques ou scientifiques (...) et à des fins d'archivage dans l'intérêt public (...) devrait également respecter d'autres dispositions pertinentes, telles que celles relatives aux essais cliniques. Le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques et à des fins d'archivage dans l'intérêt public (...) ne devrait pas être considéré comme incompatible avec les finalités pour lesquelles les données ont été initialement collectées et peut être réalisé à ces fins pendant une période plus longue que celle qui était nécessaire pour la finalité initiale (...). Les États membres devraient être autorisés à prévoir, dans des conditions spécifiques et en présence de garanties appropriées pour les personnes concernées, des dispositions précises et des dérogations concernant les exigences en matière d'information et les droits d'accès, de rectification et d'effacement, les droits à l'oubli et à la limitation du traitement et le droit à la portabilité des données ainsi que le droit d'opposition lorsque les données à caractère personnel sont traitées à des fins historiques, statistiques ou scientifiques et à des fins d'archivage (...). Les conditions et garanties en question peuvent comprendre des procédures spécifiques permettant aux personnes concernées d'exercer ces droits si cela est approprié eu égard aux finalités du traitement concerné, ainsi que des mesures techniques et organisationnelles visant à réduire le traitement des données à caractère personnel au minimum conformément aux principes de proportionnalité et de nécessité.

(125 *bis*) (…).

(125 *bis bis*) En combinant les informations issues des registres, les chercheurs peuvent acquérir de nouvelles connaissances d'un grand intérêt en ce qui concerne, par exemple, des maladies très répandues telles que les maladies cardiovasculaires, le cancer, la dépression, etc. Sur la base des registres, les résultats de la recherche peuvent être améliorés car ils s'appuient sur un échantillon plus large de population. Dans le cadre des sciences sociales, la recherche sur la base des registres permet aux chercheurs d'acquérir des connaissances essentielles sur l'incidence à long terme d'un certain nombre de conditions sociales telles que le chômage et l'éducation et de relier ces informations et celles relatives à d'autres conditions de vie. Les résultats de la recherche obtenus sur la base des registres fournissent des connaissances fiables et de grande qualité qui peuvent servir de base à l'élaboration et à la mise en œuvre d'une politique fondée sur la connaissance, améliorer la qualité de vie d'un certain nombre de personnes et renforcer l'efficacité des services sociaux, etc.
Pour faciliter la recherche scientifique, les données à caractère personnel peuvent être traitées à des fins scientifiques sous réserve de conditions et de garanties appropriées prévues dans le droit des États membres ou celui de l'Union. Le consentement de la personne concernée ne devrait donc pas être nécessaire pour chaque traitement ultérieur effectué à des fins scientifiques.

(125 *ter*) L'importance des archives pour la compréhension de l'histoire et de la culture européennes [...] et le fait que des "archives bien tenues et accessibles contribuent au fonctionnement démocratique de nos sociétés" ont été soulignés par la résolution du Conseil du 6 mai 2003 relative aux archives dans les États membres[2]. Lorsque les données à caractère personnel sont traitées à des fins d'archivage, le présent règlement devrait également s'appliquer à ce traitement, étant entendu qu'il ne devrait pas s'appliquer aux personnes décédées.

Les autorités publiques ou les organismes publics ou privés qui tiennent des registres d'intérêt public devraient être des services qui, en vertu du droit de l'Union ou d'un État membre, ont l'obligation légale d'acquérir, de préserver, d'évaluer, d'organiser, de décrire, de communiquer, de promouvoir, de diffuser des documents et d'y donner accès dans des registres présentant une utilité à long terme au regard de l'intérêt général. Les États membres devraient également être autorisés à prévoir que les données à caractère personnel peuvent faire l'objet d'un traitement ultérieur à des fins d'archivage, par exemple en vue de fournir des informations précises relatives au comportement politique dans le cadre des régimes des anciens États totalitaires.

---

[2] JO C 113 du 13.5.2003, p. 2.

Des codes de conduite peuvent contribuer à la bonne application du présent règlement, notamment lorsque des données à caractère personnel sont traitées à des fins d'archivage dans l'intérêt public en précisant davantage les garanties appropriées applicables aux droits et aux libertés de la personne concernée. Ces codes devraient être rédigés par les archives officielles des États membres ou par le Groupe européen d'Archives. Les transferts internationaux de données à caractère personnel figurant dans des archives devraient être réalisés sans préjudice de l'application des règles européennes et nationales régissant la circulation des biens culturels et des trésors nationaux.

(126) Lorsque des données à caractère personnel sont traitées à des fins scientifiques, le présent règlement devrait également s'appliquer à ce traitement. Aux fins du présent règlement, le traitement de données à caractère personnel à des fins scientifiques devrait couvrir la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé, et devrait en outre tenir compte de l'objectif de l'Union mentionné à l'article 179, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, consistant à réaliser un espace européen de la recherche. Par "fins scientifiques", il convient également d'entendre les études menées dans l'intérêt public dans le domaine de la santé publique. Pour répondre aux spécificités du traitement de données à caractère personnel à des fins scientifiques, des conditions précises devraient s'appliquer, en particulier, en ce qui concerne la publication ou la divulgation par d'autres moyens de données à caractère personnel dans le cadre de finalités scientifiques. Si le résultat de la recherche scientifique, en particulier dans le domaine de la santé, justifie de nouvelles mesures dans l'intérêt de la personne concernée, les règles générales du présent règlement s'appliquent eu égard à ces mesures.

(126 *bis*) Lorsque des données à caractère personnel sont traitées à des fins historiques, le présent règlement devrait également s'appliquer à ce traitement. Ce traitement comprend aussi les recherches historiques et les recherches à des fins généalogiques, étant entendu que le présent règlement ne devrait pas s'appliquer aux personnes décédées.

(126 *ter*) Aux fins du consentement à la participation à des activités de recherche scientifique dans le cadre d'essais cliniques (...), les dispositions pertinentes du règlement (UE) n° 536/2014 du Parlement européen et du Conseil devraient s'appliquer.

(126 *quater*) Lorsque des données à caractère personnel sont traitées à des fins statistiques, le présent règlement devrait s'appliquer à ce traitement. Le droit de l'Union ou le droit des États membres devrait, dans les limites du présent règlement, déterminer le contenu statistique, définir le contrôle de l'accès aux données et arrêter des dispositions précises pour le traitement de données à caractère personnel à des fins statistiques ainsi que des mesures appropriées pour sauvegarder les droits et les libertés de la personne concernée et garantir le secret statistique.

(126 *quinquies*) *Les informations confidentielles que les autorités nationales de la statistique et les autorités de la statistique de l'Union collectent pour élaborer des statistiques officielles européennes et nationales devraient être protégées. Les statistiques européennes devraient être mises au point, élaborées et diffusées conformément aux principes statistiques énoncés à l'article 338, paragraphe 2, du traité sur le fonctionnement de l'Union européenne, les statistiques nationales devant également être conformes au droit national. Le règlement (CE) nº 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) nº 1101/2008 du Parlement européen et du Conseil relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) nº 322/97 du Conseil relatif à la statistique communautaire et la décision 89/382/CEE, Euratom du Conseil instituant un comité du programme statistique des Communautés européennes, contient d'autres dispositions précises relatives aux statistiques européennes couvertes par le secret.*

(127) En ce qui concerne le pouvoir qu'ont les autorités de contrôle d'obtenir du responsable du traitement ou du sous-traitant l'accès aux données à caractère personnel et l'accès à ses locaux, les États membres peuvent adopter par voie législative, dans les limites du présent règlement, des règles spécifiques visant à préserver le secret professionnel ou d'autres obligations équivalentes de confidentialité, dans la mesure où cela est nécessaire pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret professionnel. Cela s'entend sans préjudice des obligations existantes incombant aux États membres en matière d'adoption du secret professionnel lorsque le droit de l'Union l'impose.

(128) Conformément à l'article 17 du traité sur le fonctionnement de l'Union européenne, le présent règlement respecte et ne préjuge pas du statut dont bénéficient, en vertu du droit constitutionnel en vigueur, les églises et les associations ou communautés religieuses dans les États membres. (...).

(129) Afin de remplir les objectifs du présent règlement, à savoir la protection des droits et libertés fondamentaux des personnes physiques, et en particulier de leur droit à la protection des données à caractère personnel, et pour garantir la libre circulation de ces dernières au sein de l'Union, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission. Concrètement, des actes délégués devraient être adoptés en ce qui concerne (…) les critères et exigences applicables aux mécanismes de certification (…) (…). Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts. Lorsque la Commission prépare et élabore des actes délégués, il convient qu'elle veille à ce que tous les documents utiles soient transmis en temps voulu, de façon appropriée et simultanée, au Parlement européen et au Conseil.

(130) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission en ce qui concerne: **(…)** des clauses contractuelles standard entre les responsables du traitement et les sous-traitants ainsi qu'entre les sous-traitants; des codes de conduite; (…) des normes techniques et des mécanismes de certification; l'adéquation du niveau de protection offert par un pays tiers, un territoire ou un secteur de traitement de données dans ce pays tiers, ou une organisation internationale; l'adoption de clauses standard en matière de protection des données; les formats et les procédures pour l'échange d'informations entre responsables du traitement, sous-traitants et autorités de contrôle en ce qui concerne les règles d'entreprise contraignantes; **(…)** l'assistance mutuelle **(…)**; et les modalités de l'échange d'informations par des moyens électroniques entre les autorités de contrôle ainsi qu'entre les autorités de contrôle et le comité européen de la protection des données. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission. Dans ce cadre, la Commission devrait envisager des mesures spécifiques pour les micro, petites et moyennes entreprises.

(131) Compte tenu de la portée générale des actes concernés, la procédure d'examen devrait être appliquée pour l'adoption d'actes d'exécution en ce qui concerne: des clauses contractuelles standard entre les responsables du traitement et les sous-traitants ainsi qu'entre les sous-traitants; des codes de conduite; (...) des normes techniques et des mécanismes de certification; l'adéquation du niveau de protection offert par un pays tiers, un territoire ou un secteur de traitement de données dans ce pays tiers, ou une organisation internationale; l'adoption de clauses standard en matière de protection des données; les formats et les procédures pour l'échange d'informations entre responsables du traitement, sous-traitants et autorités de contrôle en ce qui concerne les règles d'entreprise contraignantes; l'assistance mutuelle **(...)**; et les modalités de l'échange d'informations par des moyens électroniques entre les autorités de contrôle ainsi qu'entre les autorités de contrôle et le comité européen de la protection des données.

(132) La Commission devrait adopter des actes d'exécution immédiatement applicables lorsque, dans des cas dûment justifiés concernant un pays tiers ou un territoire ou un secteur de traitement de données dans ce pays tiers ou une organisation internationale qui n'assure pas un niveau de protection adéquat, **[...]** des raisons d'urgence impérieuses l'exigent.

(133) Étant donné que les objectifs du présent règlement, à savoir assurer un niveau équivalent de protection des personnes physiques et la libre circulation des données dans l'ensemble de l'Union, ne peuvent pas être atteints de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé au dit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(134) La directive 95/46/CE devrait être abrogée par le présent règlement. **Les traitements déjà en cours à la date d'entrée en vigueur du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur. Toutefois, lorsque ces traitements ont lieu en conformité avec la directive 95/46/CE, les exigences du présent règlement concernant la réalisation d'études d'impact sur la protection des données et la consultation préalable de l'autorité de contrôle ne devraient pas s'appliquer aux traitements déjà en cours avant l'entrée en vigueur du présent règlement, étant donné qu'il convient de satisfaire à ces exigences, de par leur nature même, avant le traitement. Lorsqu'un tel traitement est conforme à la directive 95/46/CE, il n'est pas non plus nécessaire que la personne concernée donne à nouveau son accord pour autoriser le responsable du traitement à poursuivre le traitement après la date d'application du présent règlement.** Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de ladite directive demeurent en vigueur **jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées.**

(135) Le présent règlement devrait s'appliquer à tous les aspects de la protection des droits et libertés fondamentaux à l'égard du traitement des données à caractère personnel qui ne relèvent pas d'obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE, y compris les obligations incombant au responsable du traitement et les droits des personnes physiques. Afin de clarifier la relation entre le présent règlement et la directive 2002/58/CE, cette dernière devrait être modifiée en conséquence. Après l'adoption du présent règlement, il conviendrait de réexaminer la directive 2002/58/CE, notamment afin d'assurer la cohérence avec le présent règlement (…).

(136) (...)

(137) (...)

(138) (…).

(139) (…)

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I
DISPOSITIONS GÉNÉRALES

Article premier

Objet et objectifs

1. Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.

2. Le présent règlement protège certaines libertés et certains droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.

2 *bis*. Les États membres peuvent maintenir ou introduire des dispositions plus précises en vue d'adapter l'application des règles prévues dans le présent règlement pour ce qui est du traitement des données à caractère personnel, dans le but de respecter une obligation légale ou d'exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou dans d'autres situations particulières de traitement, prévues à l'article 6, paragraphe 1, points c) et e), en définissant plus précisément des exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, notamment dans d'autres situations particulières de traitement des données prévues au chapitre IX.

3. La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Article 2

Champ d'application matériel

1. Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. Le présent règlement ne s'applique pas au traitement de données à caractère personnel:

a) dans le cadre d'une activité n'entrant pas dans le champ d'application du droit de l'Union (…);
b) par les institutions, organes, organismes et agences de l'Union;
c) par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne;
d) par une personne physique (…) dans le cadre d'une activité (...) personnelle ou domestique;
e) par (...) des autorités publiques compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou de protection contre des menaces pour la sécurité publique et de prévention de telles menaces.

3. (...).

Article 3

Champ d'application territorial

1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement de données ou d'un sous-traitant sur le territoire de l'Union.

2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées ayant leur domicile sur le territoire de l'Union par un responsable du traitement qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes concernées; ou
b) à l'observation de leur comportement, dans la mesure où celui-ci a lieu au sein de l'Union européenne.

3. Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union, mais dans un lieu où la législation nationale d'un État membre s'applique en vertu du droit international public.

Article 4

Définitions

Aux fins du présent règlement, on entend par:

1) "données à caractère personnel": toute information concernant une personne physique identifiée ou identifiable ("personne concernée"); est réputée identifiable une personne qui peut être identifiée directement ou indirectement (…), notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation, ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

2 *bis*) (...)

3) "traitement de données à caractère personnel": toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion (…), ainsi que la limitation, l'effacement ou la destruction;

3 *bis*) "limitation du traitement": le marquage de données à caractère personnel enregistrées, en vue de limiter leur traitement futur;

3 *ter*) "pseudonymisation": le traitement de données à caractère personnel de telle façon qu'elles ne puissent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable(...).

4) "fichier": tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

5) "responsable du traitement": la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités (…) et les moyens du traitement de données à caractère personnel; lorsque les finalités (…) et les moyens du traitement sont déterminés par le droit de l'Union ou la législation d'un État membre, le responsable du traitement peut être désigné, ou les critères spécifiques applicables pour le désigner peuvent être fixés, par le droit de l'Union ou par la législation d'un État membre;

6) "sous-traitant": la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

7) "destinataire": la personne physique ou morale, l'autorité publique, le service ou tout autre organisme (...) qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires;

8) "consentement de la personne concernée": toute manifestation de volonté, libre, spécifique et informée (…) par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

9) "violation de données à caractère personnel": une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière;

10) "données génétiques": toutes les données à caractère personnel liées aux caractéristiques génétiques d'une personne physique qui sont héréditaires ou ont été acquises, **(...)** et qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne, résultant en particulier d'une analyse d'un échantillon biologique de la personne en question;

11) "données biométriques": toutes les données à caractère personnel résultant d'un traitement technique spécifique relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

12) "données concernant la santé": toute donnée relative à la santé physique ou mentale d'une personne physique qui révèle des informations sur l'état de santé de ladite personne;

12 *bis*) "profilage": toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels liés à une personne physique, notamment pour analyser et prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles ou les intérêts, la fiabilité ou le comportement, ou la localisation et les déplacements;

12 *ter*) (...)

13) "établissement principal":

- en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités (...) et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union qui a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris ces décisions est considéré comme l'établissement principal;

- en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union et, s'il ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement;

14) "représentant": toute personne physique ou morale établie dans l'Union, (…) désignée par le responsable du traitement par écrit, conformément à l'article 25, qui représente ce dernier en ce qui concerne les obligations du responsable du traitement en vertu du présent règlement (…);

15) "entreprise": toute personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris (…) les sociétés de personnes ou les associations qui exercent régulièrement une activité économique;

16) "groupe d'entreprises": une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle;

17) "règles d'entreprise contraignantes": les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre de l'Union aux transferts ou à un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises ou d'un groupe d'entreprises engagées dans une activité économique conjointe;

18) (...)

19) "autorité de contrôle": une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 46;

19 *bis*) "autorité de contrôle *concernée*":

- une autorité de contrôle qui est concernée par le traitement:

  a) parce que le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre de cette autorité de contrôle;

  b) parce que des personnes concernées résidant dans cet État membre sont sensiblement affectées par le traitement ou susceptibles de l'être; ou

  c) parce que la réclamation sous-jacente a été introduite auprès de cette autorité de contrôle;

19 *ter*) "traitement transnational de données à caractère personnel":

  a) un traitement qui se déroule dans le cadre des activités, dans plusieurs États membres, d'établissements d'un responsable du traitement ou d'un sous-traitant dans l'Union qui est établi dans plusieurs États membres; ou

  b) un traitement qui se déroule dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant dans l'Union, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres;

19 *quater*)"objection pertinente et motivée":

une objection quant à savoir s'il y a ou non violation du présent règlement ou, selon le cas, si l'action envisagée en ce qui concerne le responsable du traitement ou le sous-traitant est conforme au règlement. L'objection doit établir clairement l'importance des risques que présente le projet de décision pour ce qui est des libertés et droits fondamentaux des personnes concernées et, le cas échéant, la libre circulation des données à caractère personnel;

20) "service de la société de l'information": tout service au sens de l'article 1er, paragraphe 2, de la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information;

21) "organisation internationale": une organisation internationale et ses organismes de droit public qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux ou plusieurs pays, ou dont la création est fondée sur un tel accord;

CHAPITRE II

PRINCIPES

Article 5

Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être:

   a) traitées de manière licite, équitable et transparente au regard de la personne concernée;

   b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités; le traitement ultérieur des données à caractère personnel à des fins d'archivage dans l'intérêt public ou à des fins *scientifiques*, statistiques ou historiques n'est pas considéré, conformément à l'article 83, comme incompatible avec les finalités initiales;

   c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées (…);

   d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans délai;

   e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées (**...**); les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées à des fins d'archivage dans l'intérêt public ou à des fins *scientifiques*, statistiques ou historiques, conformément à l'article 83, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de protéger les droits et libertés de la personne concernée;

   e *bis*) traitées de manière à garantir une sécurité appropriée des données à caractère personnel.

   f) (...)

2. Le responsable du traitement est responsable du respect du paragraphe 1.

Article 6

Licéité du traitement

1. Le traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

   a) la personne concernée a consenti sans ambiguïté au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

   b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

   c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

   d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne;

   e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

   f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. (...).

2. Le traitement de données à caractère personnel qui est nécessaire à des fins d'archivage dans l'intérêt public ou à des fins historiques, statistiques ou scientifiques, est licite sous réserve également des conditions et des garanties prévues à l'article 83.

3. La base juridique du traitement visé au paragraphe 1, points c) et e), doit être définie conformément:

a) au droit de l'Union, ou

b) à la législation nationale de l'État membre à laquelle le responsable du traitement des données est soumis.

Les finalités du traitement sont établies dans cette base juridique ou, eu égard au traitement visé au paragraphe 1, point e), sont nécessaires pour l'exécution d'une mission d'intérêt public ou pour l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques permettant d'adapter l'application des règles prévues dans le présent règlement, entre autres les conditions générales concernant la licéité du traitement des données par le responsable du traitement, le type de données qui font l'objet du traitement, les personnes concernées, les entités auxquelles les données peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être, la limitations des finalités, les périodes de conservation et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, notamment dans d'autres situations particulières de traitement des données prévues au chapitre IX.

3 *bis*. Afin de vérifier si les finalités d'un traitement ultérieur (...) sont compatibles avec celles pour lesquelles les données ont été initialement collectées, le responsable du traitement tient compte, à moins que la personne concernée n'ait donné son consentement, notamment:

a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données ont été collectées et les finalités du traitement ultérieur envisagé;

b) du contexte dans lequel les données ont été collectées;

c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, conformément à l'article 9;

d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées;

e) de l'existence de garanties appropriées.

4. Lorsque la finalité du traitement ultérieur est incompatible avec celle pour laquelle les données à caractère personnel ont été collectées par le même responsable du traitement, le traitement ultérieur doit avoir pour base juridique au moins l'un des motifs mentionnés au paragraphe 1, points a) à e). Un traitement ultérieur par le même responsable du traitement à des fins incompatibles en raison d'intérêts légitimes dudit responsable du traitement ou d'un tiers est licite si ces intérêts prévalent sur les intérêts de la personne concernée.

5. (...)

Article 7

Conditions applicables au consentement

1. Dans les cas où l'article 6, paragraphe 1, point a), est applicable, le responsable du traitement est capable de démontrer que la personne concernée a donné un consentement sans ambiguïté.

1 *bis*. Dans les cas où l'article 9, paragraphe 2, point a), est applicable, le responsable du traitement est capable de démontrer que la personne concernée a donné un consentement explicite.

2. Si le consentement de la personne concernée est requis dans le contexte d'une déclaration écrite qui concerne également d'autres affaires, la demande relative au consentement doit être présentée sous une forme qui la distingue clairement (…) de ces autres affaires, d'une façon compréhensible et facilement accessible, en des termes clairs et simples.

3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement préalablement donné. La personne concernée en est informée avant de donner son consentement.

4. (...)

Article 8

Conditions applicables au consentement des enfants
en ce qui concerne les services de la société de l'information

1. Dans les cas où l'article 6, paragraphe 1, point a) est applicable, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant (...) n'est licite que si, et dans la mesure où, ce consentement est donné ou autorisé par le titulaire de la responsabilité parentale ou donné par l'enfant dans des circonstances où ce consentement est considéré comme valide par le droit de l'Union ou de l'État membre.

1 *bis*. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale, compte tenu des moyens technologiques disponibles.

2. Le paragraphe 1 n'affecte pas la législation générale des États membres en matière contractuelle, notamment les dispositions régissant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.

3. (...)

4. **(...).**

Article 9

Traitement des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion, les convictions philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques ou des données concernant la santé ou la vie sexuelle (…) sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie (…):

   a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel (…), sauf lorsque le droit de l'Union ou la législation nationale prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité et de la protection sociales, dans la mesure où ce traitement est autorisé par le droit de l'Union, par la législation nationale ou par une convention collective relevant de celle-ci prévoyant des garanties appropriées;

c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;

d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers en liaison avec ses objectifs et que les données ne soient pas divulguées à des tiers sans le consentement des personnes concernées;

e) le traitement porte sur des données à caractère personnel manifestement rendues publiques par la personne concernée (...);

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle;

g) le traitement est nécessaire pour des motifs (...) d'intérêt public, sur la base du droit de l'Union ou de la législation nationale, qui doit prévoir des mesures appropriées et spécifiques en vue de sauvegarder les intérêts légitimes de la personne concernée;

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de soins ou de traitements de santé ou sociaux ou de la gestion de systèmes et de services de soins de santé ou sociaux, sur la base du droit de l'Union, de la législation nationale ou d'un contrat conclu avec un professionnel de la santé et dans le respect des conditions et des garanties prévues au paragraphe 4;

h *bis*)(...);

h *ter*) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou la législation nationale prévoyant des mesures appropriées et spécifiques en vue de sauvegarder les droits et libertés de la personne concernée;

i) le traitement est nécessaire à des fins d'archivage dans l'intérêt public ou à des fins historiques, statistiques ou scientifiques (...) et est effectué dans le respect des conditions et des garanties prévues dans le droit de l'Union ou la législation des États membres, y compris celles visées à l'article 83.

j) (...)

3. (...)

4. *Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet, sur la base du droit de l'Union ou de la législation nationale, d'un traitement aux fins prévues au paragraphe 2, point h) (...), si ces données sont traitées par un praticien soumis au secret professionnel conformément au droit de l'Union, à la législation nationale ou aux règles arrêtées par les autorités nationales compétentes, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément à la législation nationale ou de l'Union ou aux règles arrêtées par les autorités nationales compétentes.*

4 *bis*. (...).

5. Les États membres peuvent maintenir ou introduire des dispositions plus précises en ce qui concerne les données génétiques ou liées à la santé. Cela englobe la possibilité pour les États membres de (...) prévoir de nouvelles conditions pour le traitement de telles données.

Article 9 bis

Traitement des données relatives aux condamnations ou aux infractions pénales

Le traitement des données relatives aux condamnations et aux infractions pénales ou aux mesures de sûreté connexes, sur la base de l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique, ou lorsque le traitement est autorisé par le droit de l'Union ou par la législation nationale prévoyant des garanties adéquates concernant les droits et libertés des personnes concernées. Un registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

Article 10

Traitement ne nécessitant pas l'identification

1. Si les finalités pour lesquelles des données à caractère personnel sont traitées n'imposent pas ou n'imposent plus au responsable du traitement d'identifier une personne concernée, celui-ci n'est pas tenu de conserver ou d'obtenir des informations supplémentaires ni de procéder à d'autres traitements pour identifier la personne concernée à la seule fin de respecter (…) le présent règlement. (...)

2. Lorsque, dans de tels cas, le responsable du traitement ne peut pas identifier la personne concernée, les articles 15, 16, 17, 17 *bis*, 17 *ter* et 18 ne sont pas applicables, sauf lorsque la personne concernée fournit, afin d'exercer les droits que lui confèrent ces articles, des informations complémentaires qui permettent de l'identifier.

CHAPITRE III

DROITS DE LA PERSONNE CONCERNÉE

SECTION 1

TRANSPARENCE ET MODALITÉS

Article 11

Transparence des informations et des communications

1. (...)

2. (...)

Article 12

Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée

1. Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 14 et 14 bis ainsi que pour procéder à toute communication visée aux articles 15 à 19 et à l'article 32 en ce qui concerne le traitement des données à caractère personnel de la personne concernée d'une façon compréhensible et facilement accessible, en des termes clairs et simples.
Les informations sont fournies par écrit ou par d'autres moyens, le cas échéant par voie électronique. Lorsque la personne concernée en fait la demande sous forme électronique, les informations peuvent en règle générale être fournies sous forme électronique, à moins que la personne concernée ne demande qu'il en soit autrement.
Lorsque la personne concernée en fait la demande, les informations peuvent être communiquées oralement, à condition que l'identité de la personne concernée soit démontrée.

1 *bis*. Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée en vertu des articles 15 à 19. (...) Dans les cas visés à l'article 10, paragraphe 2, le responsable du traitement ne refuse pas de donner suite à la demande de la personne concernée d'exercer les droits que lui confèrent les articles 15 à 19, à moins que le responsable du traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée.

2. Le contrôleur fournit à la personne concernée**(...)** les informations sur les mesures prises sur demande en application des articles 15 et 16 à 19, sans tarder et au plus tard dans un délai d'un mois après la réception de la demande (…). Ce délai peut être prolongé de deux mois au besoin, compte tenu de la complexité et du nombre des demandes. En cas de prolongation du délai, la personne concernée est informée, dans un délai d'un mois à compter de la réception de la demande, des raisons du report.

3. Si le responsable du traitement ne donne aucune suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle (…).

4. Les informations visées aux articles 14 et 14 bis (…) ainsi que toute communication au titre des articles 16 à 19 et de l'article 32, sont fournies gratuitement. Lorsque des demandes d'une personne concernée sont *manifestement* infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement (…) peut refuser d'y donner suite. Dans ce cas, il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

4 *bis*. Sans préjudice de l'article 10, lorsque le responsable du traitement a des doutes fondés quant à l'identité de la personne présentant la demande visée aux articles 15 à 19, il peut demander la fourniture des informations complémentaires nécessaires pour confirmer l'identité de la personne concernée.

5. (...)

6. (...)

Article 13

Droits à l'égard des destinataires

(...)

SECTION 2

INFORMATION ET ACCÈS AUX DONNÉES

Article 14

Informations à fournir lorsque des données sont collectées auprès de la personne concernée

1. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement doit fournir à cette personne (…), au moment de l'obtention des données en question, les informations suivantes:

   a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable; le responsable du traitement inclut en outre les coordonnées de l'éventuel délégué à la protection des données;

   b) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que le fondement juridique du traitement.

1 *bis*. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les autres informations qui sont nécessaires pour garantir (...) un traitement équitable et transparent, compte tenu des circonstances spécifiques et du contexte du traitement des données à caractère personnel, à savoir:

   a) (…);

   b) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;

   c) les destinataires ou les catégories de destinataires des données à caractère personnel;

   d) le cas échéant, la volonté du responsable du traitement d'effectuer un transfert de données à caractère personnel vers un destinataire d'un pays tiers ou d'une organisation internationale;

e) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel relatives à la personne concernée, la rectification ou l'effacement de celles-ci, ou une limitation de leur traitement, ainsi que du droit de s'opposer au traitement de ces données (…) et du droit à la portabilité des données;

e *bis*) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer le consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement avant le retrait de celui-ci;

f) le droit d'introduire une réclamation auprès d'une autorité de contrôle (…);

g) des précisions sur le caractère réglementaire ou contractuel de l'exigence de fourniture de données à caractère personnel, ou sur la question de savoir si cette exigence conditionne la conclusion d'un contrat, ainsi que sur la question de savoir si la personne concernée est tenue de fournir les données, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données;

(h) *l'existence d'une* prise de décision automatisée comprenant *un profilage visé à l'article 20, paragraphes 1 et 3, et des informations concernant* (…) la logique sous-jacente, *ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée*.

1 *ter*. Lorsqu'il a l'intention de traiter les données (...) à des fins autres que la finalité initiale de la collecte des données, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 1 *bis*.

2. (...)

3. (...)

4. (...)

5. Les paragraphes 1, 1 *bis* et 1 *ter* ne s'appliquent pas lorsque et dans la mesure où la personne concernée dispose déjà de ces informations.

6. (...)

7. (...)

8. (...)

Article 14 bis

Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée

1. Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable du traitement peut lui fournir les informations qui suivent:

   a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable; le responsable du traitement inclut en outre les coordonnées de l'éventuel délégué à la protection des données;

   b) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que le fondement juridique du traitement.

2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée les autres informations qui sont nécessaires pour garantir qu'elle fait l'objet d'un traitement équitable et transparent, compte tenu des circonstances spécifiques et du contexte du traitement des données à caractère personnel, à savoir:

   a) les catégories de données à caractère personnel concernées;

   b) (...)

c) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;

d) les destinataires ou les catégories de destinataires des données à caractère personnel;

d *bis*) le cas échéant, la volonté du responsable du traitement d'effectuer un transfert de données à caractère personnel vers un destinataire d'un pays tiers ou d'une organisation internationale;

e) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel relatives à la personne concernée, la rectification ou l'effacement de celles-ci ou une limitation de leur traitement, ainsi que du droit de s'opposer au traitement de ces données et du droit à la portabilité des données (...);

e *bis*) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer le consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement avant le retrait de celui-ci;

f) le droit d'introduire une réclamation auprès d'une autorité de contrôle (…);

g) la source d'où proviennent les données à caractère personnel, à moins qu'elles soient issues de sources accessibles au public;

h) *l'existence d'une* prise de décision automatisée comprenant *un profilage visé à l'article 20, paragraphes 1 et 3, et des informations concernant* (…) la logique sous-jacente, *ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée*.

3. Le responsable du traitement fournit les informations visées aux paragraphes 1 et 2:

a) dans un délai raisonnable mais ne dépassant pas un mois après la collecte, eu égard aux circonstances particulières dans lesquelles les données sont traitées, ou

b) s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les informations sont communiquées pour la première fois.

3 *bis*. Lorsqu'il a l'intention de traiter les données à des fins autres que la finalité initiale pour laquelle les données ont été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

4. Les paragraphes 1 à 3 *bis* ne s'appliquent pas lorsque et dans la mesure où:

a) la personne concernée dispose déjà de ces informations; ou

b) la fourniture de telles informations **(...)** s'avère impossible ou nécessiterait des efforts disproportionnés; en pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et les libertés ainsi que les intérêts légitimes de la *personne concernée*; ou

c) l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou la législation de l'État membre à laquelle le responsable du traitement est soumis et qui établit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée; ou

d) (...);

e) les données doivent rester confidentielles conformément à la législation de l'Union ou d'un l'État membre (...).

5. (...)

6. (...)

Article 15

Droit d'accès de la personne concernée

1. La personne concernée a le droit d'obtenir du responsable du traitement, à intervalles raisonnables et gratuitement, (...) la confirmation que des données la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations qui suivent:

   a) les finalités du traitement;

   b) (...)

   c) les destinataires ou les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales;

   d) lorsque cela est possible, la durée envisagée pendant laquelle les données à caractère personnel seront conservées;

   e) l'existence du droit de demander au responsable du traitement la rectification, l'effacement ou la limitation du traitement de données à caractère personnel relatives à la personne concernée ou de s'opposer au traitement de ces données;

   f) le droit d'introduire une réclamation auprès d'une autorité de contrôle (…);

   g) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source;

   h) dans le cas des décisions résultant d'un traitement automatisé, y compris le profilage, visées à l'article 20, paragraphes 1 et 3, l'information relative à la logique sous-jacente ainsi que l'importance et les conséquences envisagées de ce traitement.

1 *bis*. Lorsque les données à caractère personnel sont transférées vers un pays tiers ou une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées, conformément à l'article 42 relatif aux transferts.

1 *ter*. À la demande et sans frais excessifs, le responsable du traitement fournit à la personne concernée une copie des données à caractère personnel faisant l'objet d'un traitement.

2. (...)

2 *bis*. Le droit d'obtenir une copie visé au paragraphe 1 *ter* (...) ne s'applique pas lorsqu'une telle copie ne peut être fournie sans divulguer des données à caractère personnel relatives à d'autres personnes concernées ou des données confidentielles relatives au responsable du traitement. En outre, ce droit ne s'applique pas si la divulgation des données à caractère personnel est susceptible de porter atteinte aux droits de propriété intellectuelle pour ce qui relève du traitement de données à caractère personnel.

3. (...)

4. (...)

SECTION 3

RECTIFICATION ET EFFACEMENT

Article 16

Droit de rectification

1. La personne concernée a le droit d'obtenir sans tarder du responsable du traitement la rectification des données à caractère personnel la concernant qui sont inexactes. Eu égard aux finalités pour lesquelles les données ont été traitées, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris par la fourniture à cet effet (...) d'une déclaration complémentaire.

2. (...)

Article 17

Droit à l'effacement et à l'"oubli numérique "

1. Le (…) responsable du traitement est tenu d'effacer les données à caractère personnel dans les meilleurs délais, notamment en ce qui concerne les données à caractère personnel qui sont collectées lorsque la personne concernée a le statut d'enfant, et la personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant, dans les meilleurs délais, pour l'un des motifs suivants:

   a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées;

   b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), (…) et il n'existe pas d'autre motif légal au traitement des données;

   c) la personne concernée s'oppose au traitement des données à caractère personnel *en vertu de l'article 19, paragraphe 1*, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19, paragraphe 2;

d) les données ont fait l'objet d'un traitement illicite;

e) les données doivent être effacées pour respecter une obligation légale à laquelle le responsable du traitement est soumis.

1 *bis*. En outre, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant, dans les meilleurs délais, si les données ont été collectées dans le cadre de l'offre de services de la société de l'information visés à l'article 8, paragraphe 1.

(...).

2. (...).

2 bis. *Lorsqu'il (...) a rendu publiques les données à caractère personnel et est tenu de les effacer en vertu du paragraphe 1*, le responsable du traitement, en tenant compte des technologies disponibles et des coûts de mise en œuvre, *prend* des mesures raisonnables, y compris d'ordre technique, permettant d'informer les responsables qui traitent les données que la personne concernée (...) a demandé l'effacement par ces responsables de tout lien vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci.

3. Les paragraphes 1, 1 bis et 2 *bis* ne s'appliquent pas dans la mesure où (…) letraitement des données à caractère personnel 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* de *données* à caractère *personnel prévue par le droit de l'Union ou par la législation d'un État membre à laquelle 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 h *ter*), ainsi qu'à l'article 9, paragraphe 4 ;

d. à des fins d'archivage dans l'intérêt général ou à des fins *scientifiques, statistiques* et historiques (...), conformément à l'article 83 ;

e. (...)

f. (...)

g. à la constatation, à l'exercice ou à la défense de droits en justice .

4. (...)

5. (...)

Article 17 *bis*

Droit à la limitation du traitement

1. La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement des données à caractère personnel lorsque:

a) l'exactitude des données est contestée par la personne concernée, pendant un délai permettant au responsable du traitement d'en vérifier l'exactitude ;

b) le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais elles sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de ses droits en justice; ou

c) elle s'est opposée au traitement en vertu de l'article 19, paragraphe 1, en attendant qu'il ait été vérifié si les raisons légitimes du responsable du traitement priment sur celles de la personne concernée.

2. (...)

3. Lorsque le traitement des données à caractère personnel est limité en vertu du paragraphe 1, ces données ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne morale ou physique, ou encore pour des motifs importants d'intérêt public .

4. Une personne concernée qui a obtenu une limitation du traitement en vertu du paragraphe 1 (...) est informée par le responsable du traitement avant que la limitation du traitement soit levée .

5. (...)

5 *bis*. (...)

Article 17 ter

Obligation de notification en ce qui concerne la rectification, l'effacement ou la limitation

Le responsable du traitement communique à chaque destinataire à qui les données ont été communiquées toute rectification, effacement ou limitation du traitement en vertu de l'article 16, de l'article 17, paragraphe 1, et de l'article 17 bis, à moins qu'une telle communication se révèle impossible ou suppose un effort disproportionné.

Article 18

Droit à la portabilité des données

1. (...)

2. Les personnes concernées ont le droit de recevoir les données les concernant qu'elles ont communiquées au responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque:

   a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b); et

   b) le traitement est automatisé.

2 *bis*. L'exercice de ce droit s'entend sans préjudice de l'article 17. Le droit visé au paragraphe 2 ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

2 *bis bis*. Le droit visé au paragraphe 2 ne s'applique pas lorsque la divulgation des données à caractère personnel pourrait porter atteinte aux droits de propriété intellectuelle pour ce qui relève du traitement de données à caractère personnel.

3. (...)

4. (…).

SECTION 4

DROIT D'OPPOSITION ET PRISE DE DÉCISION FONDÉE SUR LE TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL (...)

Article 19

Droit d'opposition

1. La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement fondé sur l'article 6, paragraphe 1, point e) ou f), la première phrase de l'article 6, paragraphe 4, en liaison avec l'article 6, paragraphe 1, point e), ou la deuxième phrase de l'article 6, paragraphe 4.

   Le responsable du traitement *ne traite plus* les données à caractère personnel (...), à moins qu'il n'établisse l'existence de raisons impérieuses et légitimes justifiant le traitement, qui priment les intérêts ou les droits et les libertés (…) de la personne concernée, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

1 *bis*. (...)

2. Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer (…) à tout moment au traitement des données à caractère personnel la concernant en vue de cette prospection. Au plus tard au moment de la première communication avec la personne concernée, ce droit est explicitement porté à l'attention de la personne concernée (…) et est présenté clairement et séparément de toute autre information.

2 *bis*. Lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel ne sont plus traitées à ces fins.

2 *bis bis*. Lorsque des données à caractère personnel sont traitées à des fins historiques, statistiques ou scientifiques, la personne concernée peut s'opposer, pour des raisons tenant à sa situation particulière, au traitement des données à caractère personnel la concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission effectuée pour des motifs d'intérêt public.

3. (...)

4. (...)

Article 20

Décision individuelle automatisée

1. La personne concernée a le droit de ne pas être soumise à une décision (…) résultant exclusivement d'un traitement automatisé, y compris le profilage, *produisant des effets juridiques* la concernant ou l'affectant de manière sensible .

1 *bis*. Le paragraphe 1 ne s'applique pas lorsque la décision: (...)

a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement (...); ou

b) est (…) autorisée par la législation de l'Union ou d'un État membre à laquelle le responsable du traitement est soumis et qui prévoit également des mesures appropriées garantissant la sauvegarde des droits et des libertés ainsi que des intérêts légitimes de la personne concernée; ou

c) est fondé sur le consentement explicite de la personne concernée (…).

1 *ter*. Dans les cas visés au paragraphe 1 *bis*, points a) et c), le responsable du traitement met en œuvre des mesures appropriées garantissant la sauvegarde des droits et des libertés ainsi que des intérêts légitimes de la personne concernée, et en tout état de cause 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.

2. (...)

3. Les décisions visées au paragraphe 1 *bis* ne sauraient être (…) fondées sur les catégories particulières de données à caractère personnel mentionnées à l'article 9, paragraphe 1, à moins que l'article 9, paragraphe 2, points a) ou g), ne s'applique et que des mesures appropriées garantissant la sauvegarde des droits et des libertés ainsi que des intérêts légitimes de la personne concernée ne soient en place.

4. (...)

5. (...)

SECTION 5
LIMITATIONS

Article 21

Limitations

1. Le droit de l'Union ou la législation de l'État membre dont relève le responsable du traitement ou le sous-traitant peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus (...) aux articles 12 à 20 et à l'article 32, ainsi qu'à l'article 5 dans la mesure où ses dispositions correspondent aux droits et obligations prévus aux articles 12 à 20, lorsqu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour:

a *bis*) assurer la sécurité nationale;

a *ter*) garantir la défense nationale;

a) assurer la sécurité publique;

b) assurer la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière**,** ou l'exécution de sanctions pénales, ou la protection contre les menaces pour la sécurité publique et la prévention de celles-ci.

c) sauvegarder d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale, ainsi que la stabilité et l'intégrité des marchés;

c *bis*) assurer la protection de l'indépendance de la justice et des procédures judiciaires;

d) assurer la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière;

e) assurer une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a), a *bis*), a *ter*), b), c) et d);

f) garantir la protection de la personne concernée ou des droits et libertés d'autrui;

g) permettre l'exécution des demandes de droit civil.

2. Tout mesure législative visée au paragraphe 1 doit contenir des dispositions spécifiques relatives, au moins, le cas échéant, aux finalités du traitement ou des catégories de traitement, aux catégories de données à caractère personnel, à l'étendue des limitations introduites, à la détermination du responsable du traitement ou des catégories de responsables du traitement, aux périodes de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ainsi que des risques pour les droits et les libertés des personnes concernées.

CHAPITRE IV

RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT

SECTION 1
OBLIGATIONS GÉNÉRALES

Article 22

Obligations incombant au responsable de traitement

1. En tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que de la probabilité et de la gravité des risques au regard des droits et des libertés des personnes physiques, le responsable du traitement (…) met en œuvre les mesures appropriées et est à même de démontrer que le traitement des données à caractère personnel est effectué dans le respect du présent règlement.

2. (…)

2 *bis*. Lorsqu'elles sont proportionnées aux activités de traitement de données, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

2 *ter.* L'adhésion aux codes de conduite approuvés visés à l'article 38 ou un mécanisme de certification approuvé visé à l'article 39 peuvent être utilisés comme moyen de démontrer le respect des obligations incombant au responsable du traitement.

3. (…)

4. (…)

Article 23

Protection des données dès la conception et protection des données par défaut

1. (...) Compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre ainsi que *de la nature, de la portée, du contexte et des finalités du traitement* ainsi que de la probabilité et de la gravité du risque présenté par le traitement au regard des droits et des libertés des personnes physiques, les responsables du traitement appliquent (…) des mesures techniques et organisationnelles *appropriées pour l'activité de traitement menée et ses objectifs*, notamment la minimisation et la pseudonymisation, de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et (…) assure la protection des droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures appropriées pour garantir que, par défaut, seules (…) les données à caractère personnel (…) qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées; cela s'applique à la quantité de (…) données collectées, à l'étendue de leur traitement, à leur période de conservation et à leur accessibilité. Lorsque le traitement n'a pas pour finalité de fournir des informations au public, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques, sans intervention humaine.

2 *bis*. Un mécanisme de certification approuvé conformément à l'article 39 *peut être utilisé comme moyen* de démontrer le respect des exigences visées aux paragraphes 1 et 2.

3. (…)

4. (…)

Article 24

Responsables conjoints du traitement

1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement de données à caractère personnel, ils sont les responsables conjoints du traitement. Ils définissent de manière transparente, par voie d'accord, leurs obligations respectives afin de se conformer aux exigences du présent règlement, en ce qui concerne notamment (…) l'exercice des droits de la personne concernée et leurs obligations respectives quant à la communication des informations visées à l'article 14 et à l'article 14 *bis*, sauf si et dans la mesure où les obligations respectives des responsables du traitement sont définies par le droit de l'Union ou la législation de l'État membre à laquelle les responsables des données sont soumis. L'accord précise lequel des responsables conjoints sert de point de contact unique pour que les personnes concernées puissent exercer leurs droits.

2. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard et contre chacun des (...) responsables du traitement.

3. L'accord reflète dûment les rôles effectifs respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées et ses grandes lignes sont mises à disposition de la personne concernée. Le paragraphe 2 ne s'applique pas lorsqu'il a été indiqué à la personne concernée, de manière transparente et sans ambiguïté, lequel des responsables conjoints a procédé au traitement, sauf si cet accord autre qu'un accord déterminé par le droit de l'Union ou la législation d'un État membre est abusif au regard des droits de la personne concernée (...).

Article 25

Représentants des responsables du traitement qui ne sont pas établis dans l'Union

1. Lorsque l'article 3, paragraphe 2, s'applique, le responsable du traitement désigne par écrit un représentant dans l'Union.

2. Cette obligation ne s'applique pas:

a) (…); ou

b) *au traitement qui est* occasionnel et *peu susceptible de constituer un* (...) *risque au regard des droits et des libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement* (...);

c) à une autorité ou à un organisme publics;

d) (…)

3. Le représentant est établi dans l'un des États membres dans lesquels résident les personnes physiques dont les données à caractère personnel sont traitées dans le contexte de l'offre de biens ou de services qui leur est proposée ou dont le comportement est observé.

3 *bis*. Le représentant est mandaté par le responsable du traitement afin d'être consulté en complément ou à la place du responsable du traitement, notamment par les autorités de contrôle et les personnes concernées, sur toutes les questions relatives au traitement de données à caractère personnel, aux fins d'assurer le respect du présent règlement.

4. La désignation d'un représentant par le responsable du traitement est sans préjudice d'actions en justice qui pourraient être intentées contre le responsable du traitement lui-même.

Article 26

Sous-traitant

1. (…). Le responsable du traitement fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes de mise en œuvre des mesures techniques et organisationnelles appropriées (…), de manière à ce que le traitement soit conforme aux prescriptions du présent règlement (…).

1 *bis*. Le sous-traitant ne recrute pas un autre sous-traitant sans l'accord écrit préalable, spécifique ou général, du responsable du traitement. Dans ce cas, le sous-traitant devrait toujours informer le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

1 *ter*. (…).

2. La réalisation d'un traitement par un sous-traitant est régie par un contrat ou **un** acte juridique au titre du droit de l'Union ou du droit national liant le sous-traitant au responsable du traitement, définissant l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, les droits du responsable du traitement (...) et prévoyant notamment que le sous-traitant:

a) ne traite les données à caractère personnel que sur instruction du responsable du traitement (…), à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou de la législation de l'État membre à laquelle le responsable du traitement est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement des données, sauf si la loi interdit une telle information pour des motifs importants d'intérêt public;

b) (…)

c) prend toutes les mesures (…) requises en vertu de l'article 30;

d) respecte les conditions de recrutement d'un autre sous-traitant (…), telles que l'obligation d'une autorisation préalable spécifique du responsable du traitement;

e) (…), compte tenu de la nature du traitement, aide le responsable du traitement à donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III;

f) (...) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 30 à 34;

g) renvoie ou supprime les données à caractère personnel, selon le choix du responsable du traitement, au terme des services de traitement des données précisés dans le contrat ou dans un autre acte juridique, à moins que le droit de l'Union ou celui de l'État membre auquel le sous-traitant est soumis exige la conservation des données;

h) met à la disposition du responsable du traitement (…) toutes les informations nécessaires pour apporter la preuve du respect des obligations prévues par le présent article, permettre la réalisation d'audits par le responsable du traitement et contribuer à ces audits.

Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou des dispositions de l'Union ou des États membres relatives à la protection des données.

2 *bis*. Lorsqu'un sous-traitant recrute (...) un autre sous-traitant pour exécuter des opérations de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations que celles fixées dans le contrat ou l'autre acte juridique liant le sous-traitant au responsable du traitement, visé au paragraphe 2, s'imposent à cet autre sous-traitant *par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit national,* en particulier pour ce qui est de présenter des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées, de manière à ce que le traitement soit conforme aux prescriptions du présent règlement. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations.

2 bis bis *L'adhésion du sous-traitant à un code de conduite approuvé visé à l'article 38 ou* un *mécanisme de certification* approuvé *visé à l'article 39* peuvent être utilisés comme moyen de démontrer l'existence *des garanties suffisantes visées aux paragraphes 1 et 2 bis*.

2 *bis ter*. Sans préjudice d'un contrat particulier entre le responsable du traitement et le sous-traitant, le contrat ou l'autre acte juridique visé aux paragraphes 2 et 2 *bis* peut être fondé, en tout ou en partie, sur les clauses contractuelles types visées aux paragraphes 2 *ter* et 2 *quater* ou sur des clauses contractuelles types qui font partie d'une certification délivrée au responsable du traitement ou au sous-traitant conformément aux articles 39 et 39 *bis*.

2 ter. La Commission peut établir des clauses contractuelles types pour les questions visées aux paragraphes 2 et 2 *bis*, conformément à la procédure d'examen visée à l'article 87, paragraphe 2.

2 *quater*. Une autorité de contrôle peut adopter des clauses contractuelles types pour les questions visées aux paragraphes 2 et 2 *bis*, conformément au mécanisme de contrôle de la cohérence visé à l'article 57.

3. Le contrat ou autre acte juridique visé aux paragraphes 2 et 2 *bis* est écrit, y compris en format électronique.

4. (…)

5. (…)

Article 27

Traitement effectué sous l'autorité du responsable du traitement et du sous-traitant

(…)

Article 28

Registre des catégories d'activités de traitement des données à caractère personnel

1. Chaque responsable du traitement et (…), le cas échéant, le représentant du responsable du traitement, tiennent un registre de toutes les catégories d'activités de traitement de données à caractère personnel mises en œuvre sous leur responsabilité. Ce registre comporte (…) les informations suivantes:

   a) le nom et les coordonnées du responsable du traitement et de tout responsable conjoint du traitement (…), du représentant du responsable du traitement et, le cas échéant, du délégué à la protection des données;

   b) (…)

   c) les finalités du traitement, y compris les intérêts légitimes, lorsque le traitement se fonde sur l'article 6, paragraphe 1, point f);

   d) une description des catégories de personnes concernées et des catégories de données à caractère personnel s'y rapportant;

   e) les (…) catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier lorsque les destinataires sont établis dans des pays tiers;

f) le cas échéant, les catégories de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale (…);

g) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;

h) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 30, paragraphe 1.

2 *bis*. Chaque sous-traitant tient un registre de toutes les catégories de traitements de données à caractère personnel effectués pour le compte du responsable du traitement, comprenant:

a) le nom et les coordonnées du sous-traitant ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, le nom et les coordonnées du représentant du responsable du traitement;

b) le nom et les coordonnées du délégué à la protection des données, le cas échéant;

c) les catégories de traitements effectués pour le compte de chaque responsable du traitement;

d) le cas échéant, les catégories de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale;

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 30, paragraphe 1.

3 *bis*. Les registres visés aux paragraphes 1 et 2 *bis* se présentent sous une forme écrite, y compris électronique, ou sous une autre forme non lisible pouvant être convertie en forme lisible.

3. Sur demande, le responsable du traitement et le sous-traitant ainsi que, le cas échéant, le représentant du responsable du traitement mettent le registre à la disposition (…) de l'autorité de contrôle.

4. Les obligations visées aux paragraphes 1 et 2 *bis* ne s'appliquent pas:

a) (…);

b) aux entreprises ou organismes comptant moins de 250 salariés, sauf si le traitement qu'ils effectuent est susceptible de comporter un risque élevé au regard des droits et des libertés des personnes concernées, par exemple (...) une discrimination, un vol ou une usurpation d'identité, un renversement non autorisé de la pseudonymisation, une perte financière, une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social pour les personnes concernées, compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

5. (…)

6. (…)

Article 29

Coopération avec l'autorité de contrôle

(…)

SECTION 2 SÉCURITÉ DES DONNÉES

Article 30

Sécurité des traitements

1. Compte tenu des techniques disponibles et des coûts liés à la mise en œuvre et prenant en considération la nature, la portée, le contexte et les finalités du traitement ainsi que la probabilité et la gravité du risque pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées, notamment (...) la pseudonymisation de données à caractère personnel, afin de garantir un niveau de sécurité approprié au regard du risque.

1 *bis*. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement des données (...), résultant notamment de la destruction accidentelle ou illégale, de la perte, de l'altération, de la divulgation ou de l'accès non autorisé à des données à caractère personnel transmises, stockées ou faisant l'objet d'un autre traitement.

2. (…)

2 *bis*. L'adhésion aux codes de conduite approuvés visés à l'article 38 ou un mécanisme de certification approuvé visé à l'article 39 peuvent être utilisés comme moyen d'*attester du respect des exigences visées au paragraphe 1*.

2 *ter*. Le responsable du traitement et le sous-traitant prennent des mesures pour que toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne puisse les traiter que sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou la législation d'un État membre.

3. (…)

4. (…)

Article 31

Notification à l'autorité de contrôle d'une violation de données à caractère personnel

1. En cas de violation de données à caractère personnel susceptible d'exposer les personnes physiques à un risque élevé au regard de leurs droits et libertés, par exemple une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social important, le responsable du traitement en adresse notification à l'autorité de contrôle compétente conformément à l'article 51, sans retard injustifié et, si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsqu'elle a lieu après ce délai de 72 heures, la notification comporte une motivation.

1 *bis*. La notification visée au paragraphe 1 n'est pas requise si une communication à la personne concernée n'est pas nécessaire aux termes de l'article 32, paragraphe 3, points a) et b).

2. (…) Le sous-traitant informe le responsable du traitement de la violation de données à caractère personnel sans retard injustifié après en avoir pris connaissance.

3. La notification visée au paragraphe 1 doit, à tout le moins:

   a) décrire la nature de la violation de données à caractère personnel y compris, si possible et s'il y a lieu, les catégories et le nombre approximatifs de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données concernés;

   b) communiquer l'identité et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

   c) (…)

   d) décrire les conséquences probables de la violation de données à caractère personnel constatée par le responsable du traitement;

e) décrire les mesures prises ou proposées par le responsable du traitement pour remédier à la violation de données à caractère personnel; et

f) le cas échéant, indiquer des mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données à caractère personnel.

3 *bis*. Si et dans la mesure où il n'est pas possible de fournir les informations visées au paragraphe 3, points d), e) et f), en même temps que les informations visées au paragraphe 3, points a) et b), le responsable du traitement fournit ces informations sans autre retard justifié.

4. Le responsable du traitement conserve une trace documentaire de toute violation de données à caractère personnel visée aux paragraphes 1 et 2, en indiquant son contexte, ses effets et les mesures prises pour y remédier. La documentation constituée doit permettre à l'autorité de contrôle de vérifier le respect des dispositions du présent article. (…)

5. (…)

6. (…)

Article 32

Communication à la personne concernée d'une violation de données à caractère personnel

1. Lorsque la violation de données à caractère personnel est susceptible d'exposer les personnes physiques à un risque élevé au regard de leurs droits et libertés , par exemple une discrimination, un vol ou une usurpation d'identité, une perte financière, une atteinte à la réputation, un renversement non autorisé de la pseudonymisation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social important, le responsable du traitement (...) en adresse notification sans retard injustifié à la personne concernée.

2. La communication à la personne concernée prévue au paragraphe 1 décrit la nature de la violation de données à caractère personnel et contient au moins les informations et recommandations prévues à l'article 31, paragraphe 3, points b), e) et f).

3. La communication (…) à la personne concernée (…), visée au paragraphe 1, n'est pas nécessaire si:

   a. le responsable du traitement (…) a mis en œuvre les mesures de protection technologiques et organisationnelles appropriées et que ces dernières ont été appliquées aux données affectées par ladite violation, en particulier celles qui rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès, telles que le cryptage; ou

   b. le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé au regard des droits et des libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser; ou

   c. elle risque d'entraîner des mesures disproportionnées, eu égard notamment au nombre de cas concernés. Dans ce cas, il convient plutôt de procéder à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace; ou

   d. elle risque de porter atteinte à un intérêt public important.

4. (…)

5. (…)

6. (…)

SECTION 3
ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES ET CONSULTATION PRÉALABLE

Article 33

Analyse d'impact relative à la protection des données

1. Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'exposer les personnes physiques à un risque élevé au regard de leurs droits et libertés, par exemple une discrimination, un vol ou une usurpation d'identité, une perte financière, une atteinte à la réputation, un renversement non autorisé de la pseudonymisation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social important, le responsable du traitement (…) effectue avant le traitement une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel. (…)

1 *bis*. Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

2. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est en particulier requise dans les cas suivants:

   a) l'évaluation systématique et à grande échelle (…) des aspects personnels propres à (…) des personnes physiques (…), qui est fondée sur le profilage et sur la base de laquelle sont prises des décisions produisant des effets juridiques concernant des personnes concernées ou affectant gravement lesdites personnes;

   b) le traitement des catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1 (...), de données biométriques ou de données se rapportant à des condamnations ou des infractions pénales, ou encore à des mesures de sûreté connexes, lorsque les données sont traitées aux fins de l'adoption de (…) décisions à grande échelle visant certaines personnes;

c) la surveillance *à grande échelle* de zones accessibles au public, en particulier lorsque des dispositifs opto-électroniques (…) sont utilisés;

d) (…);

e) (…).

2 *bis*. L'autorité de contrôle établit et publie une liste des types de traitements soumis à l'obligation d'une analyse d'impact relative à la protection des données conformément au paragraphe 1. L'autorité de contrôle communique cette liste au comité européen de la protection des données.

2 *ter*. L'autorité de contrôle peut aussi établir et publier une liste des types de traitements pour lesquels aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité européen de la protection des données.

2 *quater*. Avant d'adopter les listes visées respectivement aux paragraphes 2 *bis* et 2 *ter*, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence prévu à l'article 57, lorsque ces listes comprennent des traitements liés à l'offre de biens ou de services à des personnes concernées ou à l'observation de leur comportement dans plusieurs États membres, ou susceptibles d'affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.

3. L'analyse contient au moins une description générale des traitements envisagés, une évaluation du risque visé au paragraphe 1, les mesures envisagées pour faire face au risque y compris les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve de la conformité avec le présent règlement, en tenant compte des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées.

3 *bis*. Le respect, par les responsables du traitement ou sous-traitants compétents, des codes de conduite approuvés visés à l'article 38 est dûment pris en compte lors de l'évaluation de la légalité et de l'impact des opérations de traitement effectuées par lesdits responsables ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

4. *Le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu*, sans préjudice de la protection des intérêts généraux ou commerciaux ni de la sécurité des traitements (...).

5. (...) Lorsque le traitement visé à l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans la législation de l'État membre à laquelle le responsable du traitement est soumis, et que cette législation régit l'opération ou l'ensemble des opérations de traitement en question, les paragraphes 1 à 3 ne s'appliquent pas, sauf si les États membres estiment qu'une telle analyse est nécessaire avant le traitement.

6. (…)

7. (…)

Article 34

(…) Consultation préalable

1. (…)

2. Le responsable du traitement (…) consulte l'autorité de contrôle avant le traitement de données à caractère personnel lorsqu'une analyse d'impact relative à la protection des données telle qu'elle est prévue à l'article 33 indique que le traitement présenterait un (...) risque élevé si *le responsable du traitement ne devait pas prendre de mesures* pour atténuer le risque.

3. Lorsque l'autorité de contrôle est d'avis que le traitement visé au paragraphe 2 ne serait pas conforme au présent règlement, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué *le risque*, elle doit, dans un délai maximum de six semaines suivant la demande de consultation, conseiller le responsable du traitement de données, par écrit, et peut utiliser les pouvoirs visés à l'article 53 (...). Ce délai peut être prolongé de six semaines, compte tenu de la complexité du traitement prévu. En cas de prolongation du délai, le responsable du traitement ou le sous-traitant est informé des raisons du report, dans un délai d'un mois à compter de la réception de la demande.

4. (…)

5. (…)

6. Lorsqu'il consulte l'autorité de contrôle, conformément au paragraphe 2, le responsable du traitement (...) informe l'autorité de contrôle:

   a) le cas échéant, des responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants qui interviennent dans le traitement, en particulier pour le traitement au sein d'un groupe d'entreprises;

   b) des finalités et des modalités du traitement prévu;

   c) des mesures et des garanties prévues afin de protéger les droits et les libertés des personnes concernées conformément au présent règlement;

   d) le cas échéant, des coordonnées du délégué à la protection des données;

   e) de l'analyse d'impact relative à la protection des données prévue à l'article 33, et

   f) de toute (…) autre information demandée par l'autorité de contrôle (…).

7. Les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative qui prévoit le traitement de données à caractère personnel (...).

7 *bis*. Nonobstant le paragraphe 2, la législation des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable pour le traitement de données à caractère personnel effectué par un responsable du traitement dans le cadre d'une mission mené par celui-ci dans l'intérêt public, y compris le traitement de telles données relatives à la protection sociale et à la santé publique.

8. (…)

9. (…)

SECTION 4
DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Article 35

Désignation du délégué à la protection des données

1. Le responsable du traitement ou le sous-traitant peuvent ou doivent, si le droit de l'Union ou le droit d'un État membre l'exigent, désigner un délégué à la protection des données (…).

2. Un groupe d'entreprises peut désigner un délégué à la protection des données unique.

3. Lorsque le responsable du traitement ou le sous-traitant est une autorité ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

4. (…)

5. Le (…) délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées de la législation et des pratiques en matière de protection des données, et de sa capacité à accomplir les tâches énumérées à l'article 37, notamment l'absence de tout conflit d'intérêts. (…)

6. (…)

7. (…) Durant son mandat, sauf motifs graves au regard de la législation de l'État membre concerné justifiant le licenciement d'un employé ou d'un fonctionnaire, le délégué à la protection des données ne peut être démis de ses fonctions que s'il ne remplit plus les conditions requises pour exercer les missions qui lui incombent en vertu de l'article 37.

8. Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou accomplir ses missions sur la base d'un contrat de service.

9. Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle (…).

10. Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de données les concernant et à l'exercice des droits que leur confère le présent règlement.

11. (…)

Article 36

Fonction du délégué à la protection des données

1. Le responsable du traitement ou le sous-traitant veillent à ce que le délégué à la protection des données soit associé d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données à caractère personnel.

2. Le responsable du traitement ou le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 37 en fournissant (…) les ressources nécessaires à l'exécution de ces missions ainsi que l'accès aux données à caractère personnel et aux traitements.

3. Le responsable du traitement ou le sous-traitant veillent à ce que le délégué à la protection des données puisse agir en toute indépendance dans l'accomplissement de ses missions et ne reçoive aucune instruction en ce qui concerne l'accomplissement de celles-ci. Il ne saurait être pénalisé par le responsable du traitement ou le sous-traitant pour l'accomplissement de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé du responsable du traitement ou du sous-traitant.

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

Article 37

Missions du délégué à la protection des données

1. Les missions du (...) délégué à la protection des données (…) sont les suivantes:

   a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les salariés traitant des données à caractère personnel sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions de l'Union ou de l'État membre concerné en matière de protection des données (…);

b) contrôler la conformité au présent règlement, à d'autres dispositions de l'Union ou de l'État membre concerné en matière de protection des données et aux règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux traitements, et les audits s'y rapportant;

c) (…)

d) (…)

e) (…)

f) dispenser des conseils, lorsque cela est demandé, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution des tâches conformément à l'article 33;

g) vérifier qu'il a été répondu aux demandes de l'autorité de contrôle et, dans le domaine de compétence du délégué à la protection des données, coopérer avec l'autorité de contrôle, à la demande de celle-ci ou à l'initiative du délégué à la protection des données;

h) faire office de point de contact pour l'autorité de contrôle sur les questions liées au traitement de données à caractère personnel, y compris la consultation préalable visée à l'article 34, et consulter celle-ci, le cas échéant, sur tout autre sujet .

2. (…)

2 *bis*. Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement eu égard à la *nature, à la portée, au contexte et aux finalités* du traitement.

SECTION 5
CODES DE CONDUITE ET CERTIFICATION

Article 38

Codes de conduite

1. Les États membres, les autorités de contrôle, le comité européen de la protection des données et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des différents secteurs de traitement de données et des besoins spécifiques des micro, petites et moyennes entreprises, à la bonne application des dispositions du présent règlement.

1 *bis*. Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou en proroger la validité, afin de préciser les modalités d'application des dispositions du présent règlement, telles que:

a) le traitement loyal et transparent des données;

a *bis*) les intérêts légitimes défendus par les responsables du traitement dans des contextes spécifiques;

b) la collecte des données;

b *bis*) la pseudonymisation des données à caractère personnel;

c) l'information du public et des personnes concernées;

d) l'exercice des droits des personnes concernées;

e) l'information et la protection des enfants et la manière de recueillir le consentement des parents et des tuteurs de l'enfant;

e *bis*) les mesures et les procédures visées aux articles 22 et 23 et les mesures visant à assurer la sécurité du traitement visé à l'article 30;

ef) la notification aux autorités de contrôle des violations de données à caractère personnel et la communication à la personne concernée de ces violations;

f) (…)

1 *bis ter.* Outre l'adhésion du responsable du traitement ou du sous-traitant soumis au règlement, les codes de conduite *approuvés* en application du paragraphe 2 peuvent aussi être appliqués par des responsables du traitement ou des sous-traitants qui ne sont pas soumis au présent règlement conformément à l'article 3, afin de fournir les garanties appropriées dans le cadre des transferts de données à caractère personnel à un pays tiers ou à une organisation internationale conformément aux conditions visées à l'article 42, paragraphe 2, point d). Ces responsables du traitement ou sous-traitants prennent l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'une autre manière, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

1 *ter*. Ce code de conduite comprend les mécanismes permettant à l'organisme visé à l'article 38 bis , paragraphe 1, de procéder au contrôle obligatoire du respect de ses dispositions par les responsables du traitement ou les sous-traitants qui s'engagent à l'appliquer, sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente au titre de l'article 51 ou de l'article 51 bis .

2. Les associations et les autres organismes visés au paragraphe 1 *bis* qui ont l'intention d'élaborer un code de conduite ou de modifier ou proroger un code de conduite existant soumettent le projet de code à l'autorité de contrôle qui est compétente au titre de l'article 51. L'autorité de contrôle rend un avis sur la conformité au présent règlement du projet de code de conduite, de la modification ou de la prorogation du code existant, et approuve ce projet de code de conduite, cette modification ou cette prorogation du code existant si elle estime qu'il fournit des garanties appropriées suffisantes.

2 *bis*. Lorsque l'avis visé au paragraphe 2 confirme que le code de conduite ou le code modifié ou prorogé est conforme au présent règlement et que le code est approuvé, et s'il ne concerne pas des traitements mis en œuvre dans plusieurs États membres, l'autorité de contrôle enregistre le code de conduite et en publie les références.

2b. Si le projet de code de conduite concerne des traitements mis en œuvre dans plusieurs États membres, l'autorité de contrôle compétente au titre de l'article 51 le soumet, avant approbation, suivant la procédure visée à l'article 57, au comité européen de la protection des données, qui donne un avis sur la conformité au présent règlement du projet de code de conduite, de la modification ou de la prorogation du code existant ou, dans la situation visée au paragraphe 1 *bis ter*, sur la fourniture de garanties appropriées.

3. Si l'avis visé au paragraphe 2 *ter* confirme que le code de conduite ou le code modifié ou prorogé est conforme au présent règlement ou, dans la situation visée au paragraphe 1 *bis ter*, fournit des garanties appropriées, le comité européen de la protection des données soumet son avis à la Commission .

4. La Commission peut adopter des actes d'exécution afin de constater par voie de décision que les codes de conduite approuvés ainsi que les modifications ou prorogations de codes de conduite existants approuvés qui lui ont été soumis en vertu du paragraphe 3 sont d'application générale sur le territoire de l'Union. Les actes d'exécution sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

5. La Commission assure une publicité appropriée aux codes approuvés dont elle a constaté par voie de décision qu'ils étaient d'application générale conformément au paragraphe 4 .

5 *bis*. Le comité européen de la protection des données recueille tous les codes de conduite approuvés ainsi que les modifications qui y ont été apportées dans un registre et les met à la disposition du public par tout moyen approprié, comme le portail européen e-Justice.

Article 38 bis

Suivi des codes de conduite approuvés

1. Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente au titre des articles 52 et 53, le contrôle du respect du code de conduite visé à l'article 38, paragraphe 1 *ter*, peut être effectué par un organisme disposant d'un niveau d'expertise approprié au regard de l'objet du code agréé à cette fin par l'autorité de contrôle compétente.

2. Un organisme visé au paragraphe 1 peut être agréé à cette fin si:

a) il a prouvé, à la satisfaction de l'autorité de contrôle compétente, son indépendance et l'expertise dont il dispose au regard de l'objet du code;

b) il a établi des procédures qui lui permettent d'apprécier si les responsables du traitement ou les sous-traitants satisfont aux conditions pour appliquer le code, de contrôler le respect des dispositions dudit code et d'examiner son fonctionnement périodiquement;

c) il a établi des procédures et des structures pour traiter les réclamations relatives aux violations du code ou à la manière dont le code a été ou est appliqué par un responsable du traitement ou un sous-traitant, et rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public;

d) il prouve, à la satisfaction de l'autorité de contrôle compétente, que ses tâches et ses missions n'entraînent pas de conflit d'intérêt.

3. L'autorité de contrôle compétente soumet le projet relatif aux critères d'agrément d'un organisme visé au paragraphe 1 au comité européen de la protection des données conformément au mécanisme de contrôle de la cohérence visé à l'article 57.

4. Sans préjudice des dispositions du chapitre VIII, un organisme visé au paragraphe 1 peut, sous réserve des garanties requises, prendre des mesures appropriées en cas de violation du code par un responsable du traitement ou un sous-traitant, y compris suspendre ou exclure le responsable du traitement ou le sous-traitant concerné de l'application du code. Il informe l'autorité de contrôle compétente de ces mesures et des raisons pour lesquelles elles ont été prises.

5. L'autorité de contrôle compétente révoque l'agrément d'un organisme visé au paragraphe 1 si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organisme ne sont pas conformes au présent règlement.

6. Le présent article ne s'applique pas au traitement de données à caractère personnel effectué par les autorités et les organismes publics.

Article 39

Certification

1. Les États membres, le comité européen de la protection des données et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de marques et de labels en matière de protection des données, aux fins d'attester de la conformité au présent règlement des traitements effectués par les responsables du traitement et les sous-traitants. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération.

1 *bis*. Outre l'adhésion des responsables du traitement ou des sous-traitants soumis au présent règlement, les mécanismes de certification, les marques ou les labels en matière de protection des données *approuvés* en application du paragraphe 2 *bis* peuvent aussi être établis aux fins de démontrer l'existence de garanties appropriées fournies par des responsables du traitement ou des sous-traitants qui ne sont pas soumis au présent règlement en vertu de l'article 3, dans le cadre des transferts de données à caractère personnel à un pays tiers ou à une organisation internationale conformément aux conditions visées à l'article 42, paragraphe 2, point e). Ces responsables du traitement ou sous-traitants prennent l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'une autre manière, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

2. Une certification au titre du présent article ne diminue par la responsabilité du responsable du traitement ou du sous-traitant quant au respect du présent règlement et est sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 bis .

2 *bis*. Une certification au titre du présent article est délivrée par *les organismes* de certification *visés à l'article 39 bis ou, le cas échéant, par l'autorité de contrôle compétente* sur la base des critères approuvés par l'autorité de contrôle compétente ou, *en application de l'article 57*, par le comité européen de la protection des données.

3. Le responsable du traitement ou le sous-traitant qui soumet son traitement au mécanisme de certification fournit à l'organisme de certification visé à l'article 39 *bisou, le cas échéant, à l'autorité de contrôle compétente* toutes les informations nécessaires et lui donne accès aux activités de traitement qui sont nécessaires pour mener la procédure de certification.

4. La certification est délivrée à un responsable du traitement ou à un sous-traitant pour une période maximale de trois ans et peut être renouvelée dans les mêmes conditions tant que les exigences applicables continuent d'être respectées. Elle est retirée par les organismes de certification visés à l'article 39 *bis* ou, le cas échéant, par l'autorité de contrôle compétente lorsque les exigences applicables à la certification ne sont pas ou plus respectées.

5. Le comité européen de la protection des données recueille dans un registre tous les mécanismes de certification et les marques en matière de protection des données et les met à la disposition du public par tout moyen approprié, comme le portail européen e-Justice.

Article 39 bis

Organisme et procédure de certification

1. Sans préjudice des missions et pouvoirs de l'autorité de contrôle compétente au titre des articles 52 et 53, la certification est délivrée et renouvelée par un organisme de certification disposant d'un niveau d'expertise approprié en matière de protection des données. Chaque État membre prévoit si ces organismes de certification sont agréés par:

   a) l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 *bis*; et/ou

   b) l'organisme national d'accréditation désigné conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits, conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 *bis*.

2. L'organisme de certification visé au paragraphe 1 peut être agréé à cette fin seulement si:

   a) il a prouvé, à la satisfaction de l'autorité de contrôle compétente, son indépendance et l'expertise dont il dispose au regard de l'objet de la certification;

a *bis*) il s'est engagé à respecter les critères *visés à l'article 39, paragraphe 2 bis*, et approuvés par l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 *bis* ou, en application de l'article 57, par le comité européen de la protection des données;

b) il a mis en place des procédures en vue de l'émission, de l'examen périodique et du retrait de marques et de labels en matière de protection des données;

c) il a établi des procédures et des structures pour traiter les réclamations relatives aux violations de la certification ou à la manière dont la certification a été ou est appliquée par un responsable du traitement ou un sous-traitant, et pour rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public;

d) il prouve, à la satisfaction de l'autorité de contrôle compétente, que ses tâches et ses missions n'entraînent pas de conflit d'intérêt.

3. L'agrément des organismes de certification visés au paragraphe 1 se fait sur la base de critères approuvés par l'autorité de contrôle qui est compétente au titre de l'article 51 ou 51 *bis* ou, *en application de l'article 57*, par le comité européen de la protection des données. *En cas d'agrément en application du paragraphe 1, point b), ces exigences complètent celles prévues dans le règlement (CE) n° 765/2008 et les règles techniques qui décrivent les méthodes et procédures des organismes de certification.*

4. L'organisme de certification visé au paragraphe 1 est chargé de procéder à l'évaluation correcte en vue de la certification [ou du retrait de cette certification], sans préjudice de la responsabilité du responsable du traitement ou du sous-traitant concernant le respect du présent règlement. L'agrément est délivré pour une période maximale de cinq ans et peut être renouvelé dans les mêmes conditions tant que l'organisme respecte les exigences.

5. L'organisme de certification visé au paragraphe 1 communique à l'autorité de contrôle compétente les raisons de la délivrance ou du retrait de la certification demandée.

6. *Les* exigences visées au paragraphe 3 et *les* critères visés à l'article 39, paragraphe 2 *bis, sont publiés par l'autorité de contrôle sous une forme aisément accessible*. Les autorités de contrôle les transmettent aussi au comité européen de la protection des données. Le comité européen de la protection des données recueille dans un registre tous les mécanismes de certification et les marques en matière de protection des données et les met à la disposition du public par tout moyen approprié, comme le portail européen e-Justice.

6 *bis*. Sans préjudice des dispositions du chapitre VIII, l'autorité de contrôle compétente ou l'organisme national d'accréditation révoque l'agrément qu'il a délivré à un organisme de certification visé au paragraphe 1 si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organisme ne sont pas conformes au présent règlement.

7. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de (…) préciser les critères et exigences à prendre en considération en ce qui concerne les mécanismes de certification en matière de protection des données visés au paragraphe 1 (...).

7 *bis*. Le comité européen de la protection des données rend un avis adressé à la Commission sur les critères et les exigences visés au paragraphe 7.

8. La Commission peut fixer des normes techniques pour les mécanismes de certification, ainsi que des marques et labels et des mécanismes en matière de protection des données, afin de promouvoir et de reconnaître les mécanismes de certification ainsi que les marques et labels en matière de protection des données. Les actes d'exécution sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

CHAPITRE V
TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL VERS DES PAYS TIERS OU DES ORGANISATIONS INTERNATIONALES

Article 40

Principe général des transferts

(...)

Article 41

Transferts assortis d'une décision relative au caractère adéquat du niveau de protection

1. Un transfert de données à caractère personnel à **(...)** un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

2. Lorsqu'elle apprécie le caractère adéquat du niveau de protection, la Commission tient compte notamment des éléments suivants:

   a) la primauté du droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente (…), tant générale que sectorielle, les règles en matière de protection des données et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une organisation internationale, qui sont respectées dans le pays tiers en question ou par l'organisation internationale en question, ainsi que l'existence de droits des personnes concernées effectifs et opposables, et un droit de recours administratif et judiciaire effectif des personnes concernées dont les données à caractère personnel sont transférées (…);

b) l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, notamment par des pouvoirs de sanction appropriés, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle de l'Union et des États membres;

c) les engagements internationaux relatifs à la protection des données à caractère personnel pris par le pays tiers ou l'organisation internationale concerné, ou d'autres obligations (...) lui incombant en raison de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

2 *bis*. Le comité européen de la protection des données rend à la Commission un avis en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers ou une organisation internationale, y compris concernant l'évaluation visant à déterminer si un pays tiers, le territoire, l'organisation internationale ou un secteur déterminé n'assure plus un niveau adéquat de protection.

3. La Commission, après avoir évalué le caractère adéquat du niveau de protection, peut constater par voie de décision qu'un pays tiers, ou un territoire ou un ou plusieurs secteurs déterminés dans le pays tiers en question, ou une organisation internationale, assure un niveau de protection adéquat au sens du paragraphe 2. **(…)**. L'acte d'exécution précise son champ d'application territorial et sectoriel et, le cas échéant, cite le nom de la ou des autorités de contrôle (indépendantes) mentionnées au paragraphe 2, point b). L'acte d'exécution est adopté conformément à la procédure d'examen visée à l'article 87, paragraphe 2.

3 *bis*. *Les décisions adoptées par la Commission en vertu de l'article 25, paragraphe 6,* **(...)** *de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation par* une décision de la Commission adoptée conformément aux dispositions du paragraphe 3 ou 5.

4. (…)

4 *bis*. La Commission contrôle le bon fonctionnement des décisions adoptées en vertu du paragraphe 3 et des décisions adoptées sur la base de l'article 26, paragraphe 6, ou de l'article 25, paragraphe 4, de la directive 95/46/CE.

5. La Commission peut constater par voie de décision qu'un pays tiers, ou un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat au sens du paragraphe 2, et peut, si nécessaire, abroger, modifier ou suspendre cette décision sans effet rétroactif. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2, ou, en cas d'extrême urgence (…), conformément à la procédure prévue à l'article 87, paragraphe 3. **(…)**

5 bis. La Commission engage des consultations avec le pays tiers ou l'organisation internationale en vue de remédier à la situation donnant lieu à la décision adoptée en vertu du paragraphe 5.

6. Une décision en vertu du paragraphe 5, est sans préjudice des transferts de données à caractère personnel vers le pays tiers, ou le territoire ou secteur déterminé dans ce pays tiers, ou à l'organisation internationale en question, mis en œuvre au titre des articles 42 à 44 (...).

7. La Commission publie au *Journal officiel de l'Union européenne* une liste des pays tiers, des territoires et secteurs déterminés dans un pays tiers et des organisations internationales à l'égard desquels des décisions ont été prises au titre des paragraphes 3, 3 bis et 5.

8. (…)

Article 42

Transferts moyennant des garanties appropriées

1. Faute de décision au titre de l'article 41, paragraphe 3, le transfert de données à caractère personnel à (...) un pays tiers ou à une organisation internationale n'est possible que si le responsable du traitement ou le sous-traitant a offert des garanties appropriées, couvrant également les transferts ultérieurs (…).

2. Les garanties appropriées visées au paragraphe 1 *peuvent* notamment être fournies (...), sans que cela n'exige une autorisation particulière d'une autorité de contrôle, par:

   oa) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics;

   a) les règles d'entreprise contraignantes visées à l'article 43; ou

   b) des clauses types de protection des données adoptées par la Commission (…) conformément à la procédure d'examen prévue à l'article 87, paragraphe 2; ou

   c) des clauses types de protection des données adoptées par une autorité de contrôle (...) et adoptées par la Commission conformément à la procédure d'examen prévue à l'article 87, paragraphe 2;

   d) un code de conduite approuvé conformément à l'article 38, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant (…) dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits de la personne concernée; ou

   e) un mécanisme de certification approuvé conformément à l'article 39, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant (…) dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits de la personne concernée.

2 *bis*. Sous réserve de l'autorisation de l'autorité de contrôle compétente, les garanties appropriées visées au paragraphe 1 peuvent aussi notamment être fournies par:

a) des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données (...) dans le pays tiers ou l'organisation internationale; ou

b) (…)

c) (…)

d) des dispositions à intégrer dans des arrangements administratifs entre autorités ou organismes publics (...).

3. (…)

4. (…)

5. (…)

5 *bis*. L'autorité de contrôle applique le mécanisme de contrôle de la cohérence dans les cas visés à l'article 57, paragraphe 2, points c bis), d), e) et f).

5 *ter*. *Les autorisations accordées par un État membre ou une autorité de contrôle en vertu de l'article 26, paragraphe 2, de la directive 95/46/CE demeurent valables jusqu'à leur modification, leur remplacement ou leur abrogation par la même autorité de contrôle. Les décisions adoptées par la Commission en vertu de l'article 26, paragraphe 4, (...) de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation par une décision de la Commission* adoptée conformément aux dispositions du paragraphe 2.

Article 43

Règles d'entreprise contraignantes

1. L'autorité de contrôle compétente *approuve des règles d'entreprise contraignantes* conformément au mécanisme de contrôle de la cohérence prévu à l'article 57, à condition:

a) qu'elles soient juridiquement contraignantes, qu'elles s'appliquent à toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, et que lesdites entités en assurent le respect;

b) qu'elles confèrent expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel;

c) qu'elles respectent les exigences prévues au paragraphe 2.

2. Les règles d'entreprise contraignantes visées au paragraphe 1 précisent au moins:

a) la structure et les coordonnées du groupe *concerné* et de chacune de ses entités;

b) le transfert ou les catégories de transferts de données, y compris les types de données à caractère personnel, le type de traitement et ses finalités, la catégorie de personnes concernées et le nom du ou des pays tiers en question;

c) leur nature juridiquement contraignante, tant interne qu'externe;

d) l'application des principes généraux de protection des données, notamment la limitation de la finalité, (...) la qualité des données, la base juridique du traitement, le traitement de catégories spéciales de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes (…) qui ne sont pas liés par les règles d'entreprise contraignantes;

e) les droits des personnes concernées en ce qui concerne le traitement de leurs données à caractère personnel et les moyens de les exercer, notamment le droit de ne pas être soumis (…) à des décisions résultant exclusivement d'un traitement automatisé, y compris le profilage, conformément à l'article 20, le droit de déposer une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres conformément à l'article 75 et d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes;

f) l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre, de l'engagement de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'Union; le responsable du traitement ou le sous-traitant ne peut être exonéré, en tout ou en partie, de cette responsabilité que s'il prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause;

g) la manière dont les informations sur les règles d'entreprise contraignantes, notamment en ce qui concerne les éléments mentionnés aux points d), e) et f), sont fournies aux personnes concernées, conformément aux articles 14 et 14 bis;

h) les missions de tout délégué à la protection des données, désigné conformément à l'article 35, ou de toute autre personne ou entité chargée de la surveillance (…) du respect des règles d'entreprise contraignantes au sein du groupe, ainsi que le suivi de la formation et du traitement des réclamations;

h *bis*) les procédures de réclamation;

i) les mécanismes mis en place au sein du groupe pour garantir que le respect des règles d'entreprise contraignantes est contrôlé. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits de la personne concernée. Les résultats de ce contrôle devraient être communiqués à la personne ou à l'entité visée au point h) et au conseil d'entreprise de l'entreprise qui exerce le contrôle ou du groupe d'entreprises et devraient pouvoir être mis à la disposition de l'autorité de contrôle compétente à sa demande;

j) les mécanismes mis en place pour communiquer et archiver les modifications apportées aux règles internes et pour communiquer ces modifications à l'autorité de contrôle;

k) le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe (…), notamment en mettant à la disposition de l'autorité de contrôle les résultats des contrôles des mesures prévues au point i);

l) les mécanismes permettant de communiquer à l'autorité de contrôle compétente toutes les obligations juridiques auxquelles une entité du groupe est soumise dans un pays tiers et qui sont susceptibles d'avoir un effet négatif considérable sur les garanties fournies par les règles d'entreprise contraignantes; et

m) la formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données à caractère personnel (...).

2 *bis*. Le comité européen de la protection des données conseille la Commission, pour les règles d'entreprise contraignantes, sur la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent.

3. (…)

4. La Commission peut, pour les règles d'entreprise contraignantes au sens du présent article, spécifier la forme de l'échange d'informations (...) entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Article 44

Dérogations pour des situations particulières

1. En l'absence d'une décision relative au caractère adéquat du niveau de protection conformément à l'article 41, paragraphe 3, ou de garanties appropriées conformément à l'article 42, y compris des règles d'entreprise contraignantes (...), un transfert ou une catégorie de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peuvent être effectués qu'à condition que:
   a) la personne concernée ait explicitement consenti au transfert envisagé, après avoir été informée que ce transfert pouvait comporter des *risques* pour elle en raison de l'absence d'une décision relative au caractère adéquat du niveau de protection et de garanties appropriées;
   b) le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée;
   c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu, dans l'intérêt de la personne concernée, entre le responsable du traitement et une autre personne physique ou morale;
   d) le transfert soit nécessaire pour des motifs importants d'intérêt public;
   e) le transfert soit nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice; ou
   f) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou d'autres personnes dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;
   g) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions du droit de l'Union ou des États membres, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues dans le droit de l'Union ou des États membres pour la consultation sont remplies dans le cas particulier;

h) le transfert, *qui* n'est pas à grande échelle ou *fréquent*, soit nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement et sur lesquels ne prévalent pas les intérêts ou droits et libertés de la personne concernée et que le responsable du traitement (...) ait évalué toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données et offert (...) sur la base de cette évaluation, des garanties appropriées au regard de la protection des données à caractère personnel.

2. Un transfert effectué en vertu du paragraphe 1, point g), ne porte pas sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre. Lorsque le registre est destiné à être consulté par des personnes qui ont un intérêt légitime, le transfert n'est effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires.

3. (…)

4. Les points a), b), c) et h) du paragraphe 1 ne sont pas applicables aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.

5. L'intérêt général visé au paragraphe 1, point d), doit être reconnu par le droit de l'Union ou la législation nationale de l'État membre dont relève le responsable du traitement. **(…)**

5 *bis*. En l'absence de décision relative au caractère adéquat du niveau de protection, le droit de l'Union ou la législation nationale de l'État membre peut, pour des motifs importants d'intérêt général, fixer expressément des limites au transfert de catégories spécifiques de données à caractère personnel vers un pays tiers ou une organisation internationale. Les États membres notifient ces dispositions à la Commission.

6. Le responsable du traitement ou le sous-traitant atteste la matérialité, dans les registres visés à l'article 28 (…), de l'évaluation et des garanties appropriées (…) offertes visées au paragraphe 1, point h.

6 *bis*. (…)

7. (…)

Article 45

Coopération internationale dans le domaine de la protection des données à caractère personnel

1. La Commission et les autorités de contrôle prennent, à l'égard des pays tiers et des organisations internationales, les mesures appropriées pour:
   a) élaborer des mécanismes de coopération internationaux efficaces destinés à faciliter l'application *effective* de la législation relative à la protection des données à caractère personnel;
   b) se prêter mutuellement assistance sur le plan international dans la mise en application de la législation relative à la protection des données à caractère personnel, notamment par (…) la transmission des réclamations, l'entraide pour les enquêtes et l'échange d'information, sous réserve de garanties appropriées pour la protection des données à caractère personnel et d'autres libertés et droits fondamentaux;
   c) associer les parties prenantes intéressées aux discussions et activités visant à promouvoir la coopération internationale dans l'application de la législation relative à la protection des données à caractère personnel;
   d) favoriser l'échange et la conservation de la législation et des pratiques en matière de protection des données à caractère personnel.

2. (…)

CHAPITRE VI
AUTORITÉS DE CONTRÔLE INDÉPENDANTES

SECTION 1
STATUT D'INDÉPENDANCE

Article 46

Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du présent règlement.

1 *bis*. Chaque autorité de contrôle contribue à l'application cohérente du présent règlement dans l'ensemble de l'Union (…). À cette fin, les autorités de contrôle coopèrent entre elles et avec la Commission conformément au chapitre VII.

2. Lorsqu'un État membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité européen de la protection des données et définit le mécanisme permettant de s'assurer du respect, par les autres autorités, des règles relatives au mécanisme de contrôle de la cohérence prévu à l'article 57.

3. Chaque État membre notifie à la Commission les dispositions de la législation qu'il adopte en vertu du présent chapitre, au plus tard à la date figurant à l'article 91, paragraphe 2, et, sans délai, toute modification ultérieure les affectant.

Article 47

Indépendance

1. Chaque autorité de contrôle *exerce* en toute indépendance les fonctions et les pouvoirs qui lui sont confiés conformément au présent règlement.

2. Dans l'exercice de leurs fonctions et de leurs pouvoirs conformément au présent règlement, le membre ou les membres de l'autorité de contrôle demeurent libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions de quiconque.

3. (…)

4. (…)

5. Chaque État membre veille à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières (…), ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses fonctions et de ses pouvoirs, notamment ceux qu'elle doit mettre en œuvre dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité européen de la protection des données.

6. Chaque État membre veille à ce que chaque autorité de contrôle dispose de ses propres agents, qui sont (…) placés sous les ordres du membre ou des membres de l'autorité de contrôle.

7. Les États membres veillent à ce que chaque autorité de contrôle soit soumise à un contrôle financier qui ne menace pas son indépendance. Les États membres veillent à ce que chaque autorité de contrôle dispose d'un budget annuel public propre, pouvant faire partie du budget général de l'État ou du budget national.

Article 48

Conditions générales applicables aux membres de l'autorité de contrôle

1. Chaque État membre prévoit que le membre ou les membres de chaque autorité de contrôle doivent être nommés (...) par le parlement et/ou par le gouvernement ou le chef d'État de l'État membre concerné ou par un organisme indépendant chargé par la législation de l'État membre de procéder à la nomination selon une procédure transparente.

2. Le membre ou les membres ont les qualifications, l'expérience et les compétences nécessaires pour l'exercice de leurs fonctions et de leurs pouvoirs.

3. Les fonctions des membres prennent fin à l'échéance de leur mandat, en cas de démission ou de mise à la retraite d'office, conformément à la législation de l'État membre concerné.

4. (...)

5. (…).

Article 49

Règles relatives à l'établissement de l'autorité de contrôle

1. Chaque État membre prévoit, par voie législative:

a) la création (…) de chaque autorité de contrôle;

b) les qualifications (...) requises pour exercer les fonctions de membre de l'autorité de contrôle;

c) les règles et les procédures pour la nomination du membre ou des membres de chaque autorité de contrôle (…);

d) la durée du mandat du membre ou des membres de chaque autorité de contrôle, qui ne doit pas être (…) inférieure à quatre ans, sauf pour le premier mandat suivant l'entrée en vigueur du présent règlement, qui peut être d'une durée plus courte lorsque cela est nécessaire pour protéger l'indépendance de l'autorité de contrôle au moyen d'une procédure de nominations échelonnées;

e) le caractère renouvelable ou non renouvelable du mandat du membre ou des membres de chaque autorité de contrôle et, dans l'affirmative, pour combien de mandats;

f) (...) les conditions régissant les obligations du membre ou des membres et des agents de chaque autorité de contrôle, les interdictions d'activités ou d'emplois incompatibles avec celles-ci, y compris après la cessation de leurs activités, et les règles régissant la cessation de l'emploi;

g) (…).

2. Le membre ou les membres et les agents de chaque autorité de contrôle sont soumis, conformément au droit de l'Union ou à la législation nationale, au secret professionnel concernant toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs fonctions (…) ou de leurs pouvoirs, *y compris après la cessation de leurs activités*.

Article 50

Secret professionnel

(...)

SECTION 2

COMPÉTENCE, MISSIONS ET POUVOIRS

Article 51

Compétence

1. Chaque autorité de contrôle est compétente, sur le territoire de l'État membre dont elle relève, pour accomplir les missions et exercer les pouvoirs dont elle est investie conformément au présent règlement. (...)

2. Lorsque le traitement est effectué par des autorités publiques ou des organismes privés agissant sur la base de l'article 6, paragraphe 1, point c) ou e), l'autorité de contrôle de l'État membre concerné est compétente. Dans ce cas, l'article 51 bis n'est pas applicable.

3. Les autorités de contrôle ne sont pas compétentes pour contrôler les traitements effectués par les juridictions dans l'exercice de leur fonction juridictionnelle. (…).

Article 51 bis

Compétence de l'autorité de contrôle chef de file

1. Sans préjudice de l'article 51, l'autorité de contrôle de l'établissement principal ou de l'unique établissement du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transnational de ce responsable du traitement ou de ce sous-traitant conformément à la procédure prévue à l'article 54 bis.

2. (...)

2 bis. Par dérogation au paragraphe 1, chaque autorité de contrôle est compétente pour traiter une réclamation introduite auprès d'elle ou une éventuelle violation du présent règlement, si l'objet en concerne uniquement un établissement dans son État membre ou affecte sensiblement des personnes concernées dans son État membre uniquement.

2 *ter*. Dans les cas visés au paragraphe 2 bis, l'autorité de contrôle informe sans tarder l'autorité de contrôle chef de file de la question. Dans les trois semaines suivant le moment où elle a été informée, l'autorité de contrôle chef de file décide si elle traite ou non le cas conformément à la procédure prévue à l'article 54 bis, en tenant compte du point de savoir s'il existe ou non un établissement du responsable du traitement ou du sous-traitant dans l'État membre de l'autorité de contrôle qui l'a informée. 2 quater.

2 *quater*. Si l'autorité de contrôle chef de file décide de traiter le cas, la procédure prévue à l'article 54 bis s'applique. L'autorité de contrôle qui a informé l'autorité de contrôle chef de file peut lui soumettre un projet de décision. L'autorité de contrôle chef de file tient le plus grand compte de ce projet lorsqu'elle élabore le projet de décision visé à l'article 54 bis, paragraphe 2.

2 *quinquies*. Lorsque l'autorité de contrôle chef de file décide de ne pas le traiter, l'autorité de contrôle qui l'a informée traite le cas conformément aux articles 55 et 56.

3. L'autorité de contrôle chef de file est le seul interlocuteur du responsable du traitement ou du sous-traitant pour leur traitement transnational.

4. (…).

Article 51 ter

Identification de l'autorité de contrôle compétente pour l'établissement principal

(...)

Article 51 quater

Registre à guichet unique

(…)

Article 52

Missions

1. Sans préjudice des autres missions prévues dans le cadre du présent règlement, chaque autorité de contrôle, sur son territoire:

a) contrôle l'application du présent règlement et veille au respect de celui-ci;

a *bis*) favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement des données à caractère personnel. Les activités destinées spécifiquement aux enfants font l'objet d'une attention particulière;

a *ter*) conseille, conformément à la législation nationale, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement des données à caractère personnel;

a *quater*) encourage la sensibilisation des responsables du traitement et des sous-traitants en ce qui concerne les obligations qui leur incombent en vertu du présent règlement;

a *quinquies*) fournit des informations, sur demande, à toute personne concernée sur l'exercice de ses droits découlant du présent règlement et, si nécessaire, coopère à cette fin avec les autorités de contrôle d'autres États membres;

b) traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association la représentant, conformément à l'article 73, examine l'objet de la réclamation, dans la mesure nécessaire, et informe la personne concernée ou l'organisme, l'organisation ou l'association de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire;

c) coopère avec d'autres autorités de contrôle, y compris en partageant des informations, et leur fournit une assistance mutuelle en vue d'assurer une application cohérente du présent règlement et des mesures prises pour en assurer le respect;

d) effectue des enquêtes sur l'application du présent règlement, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique;

e) suit les évolutions présentant un intérêt, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et de la communication et des pratiques commerciales;

f) adopte les clauses contractuelles types visées à l'article 26, paragraphe 2 quater;

f *bis*) établit une liste concernant l'exigence d'une analyse d'impact relative à la protection des données conformément à l'article 33, paragraphe 2 bis;

g) fournit des conseils sur les traitements visés à l'article 34, paragraphe 3;

g *bis*) encourage l'élaboration de codes de conduite conformément à l'article 38, rend un avis et approuve les codes de conduite qui fournissent des garanties suffisantes, conformément à l'article 38, paragraphe 2;

g *ter*) encourage la mise en place de mécanismes de certification ainsi que de marques et de labels en matière de protection des données, et approuve les critères de certification conformément à l'article 39, paragraphe 2 bis;

g *quater*) procède, le cas échéant, à l'examen périodique des certifications octroyées conformément à l'article 39, paragraphe 4;

h) rédige et publie les critères d'agrément d'un organisme chargé du suivi des codes de conduite conformément à l'article 38 bis et d'un organisme de certification conformément à l'article 39 bis;

h *bis*) procède à l'agrément d'un organisme chargé du suivi des codes de conduite conformément à l'article 38 bis et d'un organisme de certification conformément à l'article 39 bis;

h *ter*) autorise les clauses contractuelles visées à l'article 42, paragraphe 2 bis, point a);

i) approuve les règles d'entreprise contraignantes conformément à l'article 43;

j) contribue aux activités du comité européen de la protection des données;

k) s'acquitte de toute autre mission relative à la protection des données à caractère personnel.

2. (...)

3. (…).

4. Chaque autorité de contrôle facilite l'introduction des réclamations visées au paragraphe 1, point b), par des mesures telles que la fourniture d'un formulaire de réclamation qui peut être rempli également par voie électronique, sans que d'autres moyens de communication soient exclus.

5. L'accomplissement des missions de chaque autorité de contrôle est gratuit pour la personne concernée et pour le délégué à la protection des données, le cas échéant.

6. Lorsque les demandes sont manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif, l'autorité de contrôle peut refuser de donner suite à la demande. Il incombe à l'autorité de contrôle d'établir le caractère manifestement infondé ou excessif de la demande.

Article 53

Pouvoirs

1. Chaque État membre prévoit, par voie législative, que son autorité de contrôle dispose au moins des pouvoirs d'enquête suivants:

a) ordonner au responsable du traitement et au sous-traitant, et, le cas échéant, au représentant du responsable du traitement, de lui communiquer toute information dont elle a besoin pour l'exercice de ses missions;

a *bis*) mener des enquêtes sous la forme d'audits sur la protection des données;

a *ter*) procéder à un examen des certifications octroyées conformément à l'article 39, paragraphe 4;

b) (...)

c) (...)

d) informer le responsable du traitement ou le sous-traitant d'une violation alléguée du présent règlement;

d *bis*) obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'exercice de ses missions;

d *ter*) obtenir l'accès à tous les locaux du responsable du traitement ou du sous-traitant, notamment à toute installation ou à tout moyen de traitement, dans le respect du droit de l'Union ou du droit procédural national.

1 *bis*. (…).

1 *ter*. Chaque État membre prévoit, par voie législative, que son autorité de contrôle dispose au moins des pouvoirs suivants en matière d'adoption de mesures correctrices:

a) avertir un responsable du traitement ou un sous-traitant du fait que les traitements envisagés sont susceptibles de violer les dispositions du présent règlement;

b) rappeler à l'ordre le responsable du traitement ou le sous-traitant lorsque les traitements ont entraîné une violation des dispositions du présent règlement;

c) (…);

c *bis*) ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes d'exercice des droits présentées par la personne concernée en application du présent règlement;

d) ordonner au responsable du traitement ou au sous-traitant de mettre les traitements en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé; en particulier en ordonnant la rectification, la limitation ou l'effacement de données en application des articles 16, 17 et 17 bis et la notification de ces mesures aux destinataires auxquels les données ont été divulguées conformément à l'article 17, paragraphe 2 bis, et à l'article 17 ter;

e) limiter temporairement ou définitivement un traitement (...);

f) ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale;

g) infliger une amende administrative en application des articles 79 et 79 bis, en complément ou à la place des mesures visées au présent paragraphe, en fonction des particularités de chaque cas individuel.

1 *quater*. Chaque État membre prévoit, par voie législative, que son autorité de contrôle dispose au moins des pouvoirs d'autorisation et des pouvoirs consultatifs suivants:

a) conseiller le responsable du traitement conformément à la procédure de consultation préalable visée à l'article 34;

a *bis*) émettre, de sa propre initiative ou sur demande, des avis à l'attention du parlement national, du gouvernement de l'État membre ou, conformément à la législation nationale, d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel;

a *ter*) autoriser le traitement visé à l'article 34, paragraphe 7 bis, si la législation de l'État membre exige une telle autorisation préalable;

a *quater*) émettre un avis sur les projets de codes de conduite prévus à l'article 38, paragraphe 2 et les approuver;

a *quinquies*) agréer des organismes de certification conformément à l'article 39 bis;

a *sexies*) octroyer des certifications et approuver des critères de certification conformément à l'article 39, paragraphe 2 bis;

b) adopter les clauses types de protection des données visées à l'article 42, paragraphe 2, point c);

c) autoriser les clauses contractuelles visées à l'article 42, paragraphe 2 bis, point a);

c *bis*) autoriser les accords administratifs visés à l'article 42, paragraphe 2 bis, point d);

d) approuver les règles d'entreprise contraignantes conformément à l'article 43.

2. *L'exercice des pouvoirs conférés à l'autorité de contrôle en application du présent article est subordonné à des garanties appropriées, y compris le droit à un recours effectif et à une procédure régulière, prévues par le droit de l'Union et la législation des États membres conformément à la charte des droits fondamentaux de l'Union européenne*.

3. Chaque État membre prévoit, par voie législative, que son autorité de contrôle a le pouvoir de porter toute violation du présent règlement à la connaissance de l'autorité judiciaire et (...), le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire respecter les dispositions du présent règlement.

4. (...)

5. (...)

Article 54

Rapport d'activité

Chaque autorité de contrôle établit un rapport annuel sur son activité. Le rapport est transmis au parlement national, au gouvernement et à d'autres autorités désignées par la législation nationale. Il est mis à la disposition du public, de la Commission européenne et du comité européen de la protection des données.

CHAPITRE VII

COOPÉRATION ET COHÉRENCE

SECTION 1

COOPÉRATION

Article 54 bis

Coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées

1. L'autorité de contrôle chef de file (...) coopère avec les autres autorités de contrôle concernées conformément au présent article en vue de parvenir à un consensus (...). L'autorité de contrôle chef de file et les autorités de contrôle concernées échangent toute information utile.

1 *bis*. L'autorité de contrôle chef de file peut demander à tout moment aux autres autorités de contrôle concernées de se prêter une assistance mutuelle en application de l'article 55 et peut mener des opérations conjointes en application de l'article 56, en particulier pour effectuer des enquêtes ou contrôler l'application d'une mesures concernant un responsable du traitement ou un sous-traitant établi dans un autre État membre.

2. L'autorité de contrôle chef de file communique sans tarder les informations utiles sur la question aux autres autorités de contrôle concernées. Elle soumet sans délai un projet de décision aux autres autorités de contrôle concernées en vue d'obtenir leur avis et tient dûment compte de leurs points de vue.

3. Lorsqu'une des autres autorités de contrôle concernées formule, dans les quatre semaines suivant la consultation conformément au paragraphe 2, une objection pertinente et motivée *en ce qui concerne le projet de décision*, l'autorité de contrôle chef de file, si elle ne donne pas suite à l'objection ou si elle est d'avis que celle-ci n'est pas pertinente et motivée, soumet la question au mécanisme de contrôle de la cohérence visé à l'article 57. (...)

3 *bis*. Lorsque l'autorité de contrôle chef de file entend donner suite à l'objection formulée, elle soumet aux autres autorités de contrôle concernées un projet révisé de décision en vue d'obtenir leur avis. Ce projet révisé de décision est soumis à la procédure visée au paragraphe 3 dans un délai de deux semaines.

4. Lorsqu'aucune des autres autorités de contrôle concernées n'a formulé d'objection au projet de décision soumis par l'autorité de contrôle chef de file dans le délai visé aux paragraphes 3 et 3 bis, l'autorité de contrôle chef de file et les autorités de contrôle concernées sont réputées approuver ce projet de décision et sont liées par lui.

4 *bis*. L'autorité de contrôle chef de file adopte la décision, la communique à l'établissement principal ou à l'établissement unique du responsable du traitement ou du sous-traitant, selon le cas, et informe les autres autorités de contrôle concernées et le comité européen de la protection des données de la décision en question, y compris par un résumé des faits et motifs pertinents. L'autorité de contrôle auprès de laquelle une réclamation a été introduite informe de la décision la personne à l'origine de la réclamation.

4 *ter*. Par dérogation au paragraphe 4 bis, lorsqu'une réclamation est refusée ou rejetée, l'autorité de contrôle auprès de laquelle la réclamation a été introduite adopte la décision, la communique à la personne à l'origine de la réclamation et en informe le responsable du traitement.

4 *ter ter*. Lorsque l'autorité de contrôle chef de file et les autorités de contrôle concernées sont d'accord pour refuser ou rejeter des parties d'une réclamation et donner suite à d'autres parties de cette réclamation, une décision distincte est adoptée pour chacune de ces parties de l'affaire. L'autorité de contrôle chef de file adopte la décision pour la partie relative aux actions concernant le responsable du traitement et la communique à l'établissement principal ou à l'établissement unique du responsable du traitement ou du sous-traitant sur le territoire de l'État membre dont elle relève et en informe la personne à l'origine de la réclamation, tandis que l'autorité de contrôle de la personne à l'origine de la réclamation adopte la décision pour la partie concernant le refus ou le rejet de cette réclamation, la communique à cette personne et en informe le responsable du traitement ou le sous-traitant.

4 *quater*. Après avoir été informé de la décision de l'autorité de contrôle chef de file en application des paragraphes 4 bis et 4 ter ter, le responsable du traitement ou le sous-traitant prend les mesures nécessaires pour assurer le respect de la décision en ce qui concerne les activités de traitement menées dans le cadre de tous ses établissements dans l'Union. Le responsable du traitement ou le sous-traitant communique les mesures prises pour assurer le respect de la décision à l'autorité de contrôle chef de file, qui informe les autres autorités de contrôle concernées.

4 *quinquies*. Lorsque, dans des circonstances exceptionnelles, une autorité de contrôle concernée a des raisons de considérer qu'il est urgent d'intervenir pour protéger les intérêts des personnes concernées, la procédure d'urgence visée à l'article 61 est applicable.

5. L'autorité de contrôle chef de file et les autres autorités de contrôle concernées se communiquent mutuellement par des moyens électroniques, au moyen d'un formulaire type, les informations requises en vertu du présent article (...).

Article 54 ter

Coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées dans des cas particuliers de non-respect du règlement

(...)

Article 55

Assistance mutuelle

1. Les autorités de contrôle se communiquent toute information utile et se prêtent une assistance mutuelle en vue de mettre en œuvre et d'appliquer le présent règlement de manière cohérente et mettent en place des mesures pour coopérer efficacement. L'assistance mutuelle concerne notamment les demandes d'informations et les mesures de contrôle, telles que les demandes d'autorisation et de consultation préalables, les inspections et les enquêtes. (...)

2. Chaque autorité de contrôle prend toutes les mesures appropriées nécessaires pour répondre à la demande d'une autre autorité de contrôle, dans les meilleurs délais et au plus tard un mois après réception de la demande. Il peut s'agir notamment de la transmission d'informations utiles sur la conduite d'une enquête (...).

3. La demande d'assistance contient toutes les informations nécessaires, notamment la finalité et les motifs justifiant la demande. Les informations échangées ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

4. Une autorité de contrôle saisie d'une demande d'assistance ne peut refuser d'y donner suite, à moins:

   a) qu'elle ne soit pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter;

   b) qu'elle soit incompatible avec les dispositions du présent règlement ou du droit de l'Union ou de la législation de l'État membre à laquelle l'autorité de contrôle qui a reçu la demande est soumise.

5. L'autorité de contrôle requise informe l'autorité de contrôle requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour donner suite à la demande. Lorsqu'elle refuse de donner suite à une demande en application du paragraphe 4, elle explique les raisons de son refus.

6. Les autorités de contrôle communiquent en règle générale par des moyens électroniques, en utilisant un formulaire type, les informations demandées par d'autres autorités de contrôle.

7. Une mesure prise à la suite d'une demande d'assistance mutuelle ne donne pas lieu à la perception de frais. Les autorités de contrôle peuvent convenir, avec d'autres autorités de contrôle, de règles relatives à l'octroi, par d'autres autorités de contrôle, de dédommagements concernant des dépenses spécifiques résultant de la fourniture d'une assistance mutuelle dans des circonstances exceptionnelles.

8. Lorsqu'une autorité de contrôle ne fournit pas les informations visées au paragraphe 5, dans un délai d'un mois à compter de la réception de la demande formulée par une autre autorité de contrôle, l'autorité de contrôle requérante peut adopter une mesure provisoire sur le territoire de l'État membre dont elle relève, conformément à l'article 51, paragraphe 1, et saisit le comité européen de la protection des données (...) de l'affaire, conformément au mécanisme de contrôle de la cohérence prévu à l'article 57.

9. L'autorité de contrôle précise la durée de validité de la mesure provisoire ainsi adoptée, qui ne peut excéder trois mois. L'autorité de contrôle communique sans tarder cette mesure, en indiquant les motifs de son adoption, au comité européen de la protection des données, (…) conformément au mécanisme de contrôle de la cohérence prévu à l'article 57.

10. La Commission peut préciser la forme et les procédures de l'assistance mutuelle objet du présent article, ainsi que les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle et entre les autorités de contrôle et le comité européen de la protection des données, notamment le formulaire type mentionné au paragraphe 6. Les actes d'exécution correspondants sont adoptés en conformité avec la procédure d'examen visée à l'article 87, paragraphe 2.

Article 56

Opérations conjointes des autorités de contrôle

1. Les autorités de contrôle peuvent, le cas échéant, mener des opérations conjointes, notamment effectuer des enquêtes conjointes et prendre des mesures répressives conjointes, auxquelles participent des membres ou des agents des autorités de contrôle d'autres États membres.

2. Si le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ou si un nombre important de personnes concernées dans plusieurs États membres sont susceptibles d'être sensiblement affectées par le traitement, une autorité de contrôle de chacun de ces États membres a le droit de participer aux opérations conjointes, selon le cas. L'autorité de contrôle compétente invite l'autorité de contrôle de chacun de ces États membres à prendre part aux opérations conjointes concernées et donne suite sans tarder à toute demande d'une autorité de contrôle souhaitant y participer.

3. Une autorité de contrôle peut, conformément au droit de l'État membre dont elle relève, et avec l'accord de l'autorité de contrôle de l'État membre d'origine, confier des pouvoirs, notamment des pouvoirs d'enquête, aux membres ou aux agents de l'autorité de contrôle de l'État membre d'origine participant à des opérations conjointes ou admettre, pour autant que le droit de l'État membre dont relève l'autorité de contrôle d'accueil le permette, que les membres ou les agents de l'autorité de contrôle de l'État membre d'origine exercent leurs pouvoirs d'enquête conformément au droit de l'État membre dont relève l'autorité de contrôle d'origine. Ces pouvoirs d'enquête ne peuvent être exercés que sous l'autorité et en présence de membres ou d'agents de l'autorité de contrôle de l'État membre d'accueil. Les membres ou agents de l'autorité de contrôle de l'État membre d'origine sont soumis au droit national de l'autorité de contrôle de l'État membre d'accueil. (...)

3 *bis*. Lorsque, conformément au paragraphe 1, les agents de l'autorité de contrôle de l'État membre d'origine opèrent dans un autre État membre, l'État membre d'accueil de l'autorité de contrôle est responsable des dommages qu'ils causent au cours des opérations dont ils sont chargés, conformément au droit de l'État membre sur le territoire duquel ils opèrent.

3 *ter*. L'État membre sur le territoire duquel des dommages ont été causés assume la réparation de ces dommages dans les conditions applicables aux dommages causés par ses propres agents. L'État membre d'origine de l'autorité de contrôle dont les agents ont causé des dommages à toute personne sur le territoire d'un autre État membre rembourse intégralement à ce dernier les sommes qu'il a versées à leurs ayants droit.

3 *quater*. Sans préjudice de l'exercice de ses droits à l'égard des tiers et par dérogation au paragraphe 3 ter, chaque État membre renonce, dans le cas prévu au paragraphe 1, à demander à un autre État membre le remboursement du montant des dommages qu'il a subis.

4. (...)

5. Lorsqu'une opération conjointe est envisagée et qu'une autorité de contrôle ne se conforme pas, dans un délai d'un mois, à l'obligation énoncée au paragraphe 2, deuxième phrase, les autres autorités de contrôle peuvent adopter une mesure provisoire sur le territoire de leur État membre, conformément à l'article 51, paragraphe 1.

6. L'autorité de contrôle précise la durée de validité des mesures provisoires prévues au paragraphe 5, qui ne peut excéder trois mois. L'autorité de contrôle communique sans tarder cette mesure, en indiquant les motifs de son adoption, au comité européen de la protection des données, (…) conformément au mécanisme de contrôle de la cohérence prévu à l'article 57.

SECTION 2

COHÉRENCE

Article 57

Mécanisme de contrôle de la cohérence

1. Aux fins visées à l'article 46, paragraphe 1 bis, les autorités de contrôle coopèrent entre elles dans le cadre du mécanisme de contrôle de la cohérence établi dans la présente section.

2. Le comité européen de la protection des données émet un avis chaque fois qu'une *autorité de contrôle* compétente envisage *d'adopter* l'une des mesures ci-après (...). À cet effet, l'autorité de contrôle compétente communique le projet de décision au comité européen de protection des données, lorsque ce projet:

   a) (…);

   b) (…);

   c) vise à adopter une liste de traitements soumis à l'exigence d'une analyse d'impact relative à la protection des données conformément à l'article 33, paragraphe 2 ter;

   c *bis*) concerne la question de savoir, au titre de l'article 38, paragraphe 2 ter, si un code de conduite, la modification ou la prorogation d'un code de conduite sont conformes au présent règlement;

   c *ter*) vise à approuver les critères d'agrément d'un organisme, conformément à l'article 38 bis, paragraphe 3, ou d'un organisme de certification, conformément à (...) l'article 39 bis, paragraphe 3;

d) vise à fixer des clauses types de protection des données telles que celles visées à l'article 42, paragraphe 2, point c);

e) vise à autoriser les clauses contractuelles visées à l'article 42, paragraphe 2, point d); ou

f) vise à approuver des règles d'entreprise contraignantes au sens de l'article 43.

3. Le comité européen de la protection des données adopte une décision contraignante dans les cas suivants:

a) lorsque, dans un cas visé à l'article 54 bis, paragraphe 3, une autorité de contrôle concernée a formulé une objection pertinente et motivée à un projet de décision de l'autorité chef de file ou que l'autorité chef de file a rejeté une objection comme étant non pertinente et/ou non motivée. La décision contraignante concerne toutes les questions qui font l'objet de l'objection pertinente et motivée, notamment celle de savoir s'il y a infraction au règlement;

b) lorsqu'il existe des points de vue divergents quant à l'autorité de contrôle concernée compétente pour l'établissement principal;

c) (...)

d) lorsqu'une autorité de contrôle compétente ne demande pas l'avis du comité européen de la protection des données dans les cas visés au paragraphe 2 ou qu'elle ne suit pas l'avis émis par le comité européen de la protection des données en vertu de l'article 58. Dans ce cas, toute autorité de contrôle concernée ou la Commission peut saisir le comité européen de la protection des données.

4. Toute autorité de contrôle, le président du comité européen de la protection des données ou la Commission peuvent demander que toute question d'application générale ou produisant des effets dans plusieurs États membres soit examinée par le comité européen de la protection des données en vue d'obtenir un avis, en particulier lorsqu'une autorité de contrôle compétente ne respecte pas les obligations relatives à l'assistance mutuelle découlant de l'article 55 ou les obligations relatives aux opérations conjointes découlant de l'article 56.

5. Les autorités de contrôle et la Commission communiquent au comité européen de la protection des données, par voie électronique et au moyen d'un formulaire type, toutes les informations utiles, notamment, selon le cas, un résumé des faits, le projet de décision, les motifs rendant nécessaire l'adoption de cette mesure et les points de vue des autres autorités de contrôle concernées.

6. Le président du comité européen de la protection des données transmet, dans les meilleurs délais, aux membres de ce comité et à la Commission, toutes les informations utiles qui lui ont été communiquées, par voie électronique et au moyen d'un formulaire type. Le secrétariat du comité européen de la protection des données fournit, si nécessaire, les traductions des informations utiles.

Article 58

Avis du comité européen de la protection des données

1. (...)

2. (...)

3. (...)

4. (...)

5. (...)

6. (...)

7. Dans les cas visés à l'article 57, paragraphes 2 et 4, le comité européen de la protection des données émet un avis sur la question qui lui est soumise, à condition qu'il n'ait pas déjà émis d'avis sur la même question. Cet avis est adopté dans un délai d'un mois à la majorité simple des membres du comité européen de la protection des données. Ce délai peut être prolongé d'un mois, en fonction de la complexité de la question. En ce qui concerne le projet de décision transmis aux membres du comité conformément à l'article 57, paragraphe 6, un membre qui n'a pas formulé d'objection dans le délai indiqué par le président est réputé approuver le projet de décision.

7 *bis*. Au cours de la période visée au paragraphe 7, l'autorité de contrôle compétente n'adopte pas son projet de décision conformément à l'article 57, paragraphe 2.

7 *ter*. Le président du comité européen de la protection des données informe de l'avis, dans les meilleurs délais, l'autorité de contrôle visée, selon le cas, à l'article 57, paragraphes 2 et 4, et la Commission, et le publie.

8. L'autorité de contrôle visée à l'article 57, paragraphe 2, tient le plus grand compte de l'avis du comité européen de la protection des données et fait savoir par voie électronique au président du comité européen de la protection des données, dans un délai de deux semaines à compter de la réception de l'avis, si elle maintient ou si elle modifiera le projet de décision, et, le cas échéant, communique, au moyen d'un formulaire type, le projet de décision modifié.

9. Lorsque l'autorité de contrôle concernée informe le président du comité européen de la protection des données dans le délai visé au paragraphe 8, qu'elle n'a pas l'intention de suivre, en tout ou en partie, l'avis du comité en fournissant des motifs pertinents, l'article 57, paragraphe **3**, est applicable.

10. (...)

11. (...)

Article 58 bis

Décisions du comité européen de la protection des données

1. Dans les cas visés à l'article 57, paragraphe 3, le comité européen de la protection des données adopte une décision sur la question qui lui est soumise en vue d'assurer l'application correcte et cohérente du présent règlement dans différentes situations. La décision, motivée, est adressée à l'autorité de contrôle chef de file ainsi qu'à toutes les autorités de contrôle concernées, qui sont liées par cette décision.

2. La décision visée au paragraphe 1 est adoptée à la majorité des deux tiers des membres du comité dans un délai d'un mois à compter de la transmission de la question. Ce délai peut être prolongé d'un mois en fonction de la complexité de la question.

3. Si le comité n'a pas été en mesure d'adopter une décision dans les délais visés au paragraphe 2, il adopte sa décision, à la majorité simple de ses membres, dans un délai de deux semaines à compter de l'expiration du deuxième mois visé au paragraphe 2. En cas de division des membres du comité, la décision est adoptée par vote de son président.

4. Les autorités de contrôle concernées n'adoptent pas de décision sur la question soumise au comité en vertu du paragraphe 1 au cours des périodes visées aux paragraphes 2 et 3.

5. (...)

6. Le président du comité européen de la protection des données notifie, dans les meilleurs délais, la décision visée au paragraphe 1 aux autorités de contrôle concernées. Il en informe la Commission. La décision est publiée sur le site web du comité européen de la protection des données sans délai après que l'autorité de contrôle a notifié la décision définitive visée au paragraphe 7.

7. L'autorité de contrôle chef de file ou, le cas échéant, l'autorité de contrôle auprès de laquelle la réclamation a été introduite, adopte sa décision finale sur la base de la décision visée au paragraphe 1, dans les meilleurs délais et au plus tard un mois après que le comité européen de la protection des données a notifié sa décision. L'autorité de contrôle chef de file ou, le cas échéant, l'autorité de contrôle auprès de laquelle la réclamation a été introduite, informe le comité européen de la protection des données de la date à laquelle sa décision définitive est notifiée au responsable du traitement ou au sous-traitant ainsi qu'à la personne concernée. La décision définitive des autorités de contrôle concernées est adoptée conformément à l'article 54 bis, paragraphes 4 bis, 4 ter et 4 ter ter. La décision définitive fait référence à la décision visée au paragraphe 1 et précise que celle-ci sera publiée sur le site web du comité européen de la protection des données conformément au paragraphe 6. La décision définitive est jointe à la décision visée au paragraphe 1.

Article 59

Avis de la Commission

(...)

Article 60

Suspension d'un projet de mesure

(...)

Article 61

Procédure d'urgence

1. Dans des circonstances exceptionnelles, lorsqu'une autorité de contrôle concernée considère qu'il est urgent d'intervenir pour protéger les droits et les libertés des personnes concernées, elle peut, par dérogation au mécanisme de contrôle de la cohérence prévu à l'article 57 ou à la procédure prévue à l'article 54 bis, adopter sans tarder des mesures provisoires visant à produire des effets juridiques sur le territoire de l'État membre dont elle relève et ayant une durée de validité déterminée. L'autorité de contrôle communique sans tarder ces mesures et les raisons de leur adoption, aux autres autorités de contrôle concernées, au comité européen de la protection des données et à la Commission.

2. Lorsqu'une autorité de contrôle a pris une mesure en vertu du paragraphe 1 et estime que des mesures définitives doivent être adoptées d'urgence, elle peut demander un avis d'urgence ou une décision contraignante d'urgence au comité européen de la protection des données, en motivant sa demande.

3. Toute autorité de contrôle peut, en motivant sa demande et notamment l'urgence d'intervenir, demander un avis d'urgence ou une décision contraignante d'urgence au comité européen de la protection des données, selon le cas, lorsqu'une autorité de contrôle compétente n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les droits et les libertés des personnes concernées.

4. Par dérogation à l'article 58, paragraphe 7, et à l'article 58 bis, paragraphe 2, l'avis d'urgence ou la décision contraignante d'urgence visés aux paragraphes 2 et 3 sont adoptés dans un délai de deux semaines à la majorité simple des membres du comité européen de la protection des données.

Article 62

Actes d'exécution

1. La Commission peut adopter des actes d'exécution de portée générale pour:

   a) (…);

   b) (…);

   c) (…);

   d) définir les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle, et entre ces autorités et le comité européen de la protection des données, notamment le formulaire type visé à l'article 57, paragraphes 5 et 6, et à l'article 58, paragraphe 8.

   Les actes d'exécution correspondants sont adoptés en conformité avec la procédure d'examen visée à l'article 87, paragraphe 2.

2. (...)

3. (...)

Article 63

Exécution

(...)

Section 3

Comité européen de la protection des données

Article 64

Comité européen de la protection des données

1 *bis*. Le comité européen de la protection des données est institué en tant qu'organe de l'Union et possède la personnalité juridique.

1 *ter*. Le comité européen de la protection des données est représenté par son président.

2. Le comité européen de la protection des données se compose du directeur d'une autorité de contrôle de chaque État membre ou de son représentant et du contrôleur européen de la protection des données.

3. Lorsque, dans un État membre, plusieurs autorités de contrôle sont chargées de surveiller l'application des dispositions du présent règlement, (...) un représentant commun est désigné conformément à la législation nationale de cet État membre.

4. La Commission et le contrôleur européen de la protection des données ou son représentant ont le droit de participer aux activités et réunions du comité européen de la protection des données *sans droit de vote*. La Commission désigne un représentant. Le président du comité européen de la protection des données informe (...) la Commission des activités du comité européen de la protection des données.

Article 65

Indépendance

1. Le comité européen de la protection des données accomplit les missions qui lui sont confiées ou exerce les compétences qui lui sont conférées conformément aux articles 66 et 67 en toute indépendance.

2. Sans préjudice des demandes de la Commission visées à l'article 66, paragraphe 1, point b), et paragraphe 2, le comité européen de la protection des données ne sollicite ni n'accepte d'instructions de quiconque dans l'accomplissement de ses missions ou l'exercice de ses compétences.

Article 66

Missions du comité européen de la protection des données

1. Le comité européen de la protection des données promeut l'application cohérente du présent règlement. À cet effet, le comité européen de la protection des données, de sa propre initiative ou à la demande de la Commission, a notamment pour mission:

   aa) de surveiller et garantir l'application correcte du présent règlement dans les cas prévus à l'article 57, paragraphe 3, sans préjudice des missions des autorités de contrôle nationales;

   a) de conseiller la Commission sur toute question relative à la protection des données à caractère personnel dans l'Union, notamment sur tout projet de modification du présent règlement;

b) d'examiner, de sa propre initiative, à la demande de l'un de ses membres ou à la demande de la Commission, toute question portant sur l'application du présent règlement, et de publier des lignes directrices, des recommandations et de bonnes pratiques, afin de favoriser l'application cohérente du présent règlement;

b *bis*) d'élaborer, à l'intention des autorités de contrôle, des lignes directrices concernant l'application des mesures visées à l'article 53, paragraphes 1, 1 ter et 1 quater, ainsi que la fixation des amendes administratives prévues aux articles 79 et 79 bis;

c) de faire le bilan de l'application pratique des lignes directrices, recommandations et bonnes pratiques visées aux points b) et b bis);

c *bis*) d'encourager l'élaboration de codes de conduite et la mise en place de mécanismes de certification et de marques et de labels en matière de protection des données, conformément aux articles 38 et 39;

c *ter*) de procéder à l'agrément des organismes de certification et à l'examen périodique de cet agrément conformément à l'article 39 bis et de tenir un registre public des organismes agréés conformément à l'article 39 bis, paragraphe 6, ainsi que des responsables du traitement ou des sous-traitants agréés établis dans des pays tiers conformément à l'article 39, paragraphe 4;

c *quinquies*) de définir les exigences visées à l'article 39 bis, paragraphe 3, aux fins de l'agrément des organismes de certification prévu à l'article 39;

c *sexies*) de communiquer à la Commission un avis sur le niveau de protection des données à caractère personnel dans les pays tiers ou les organisations internationales, en particulier dans les cas visés à l'article 41;

d) d'émettre des avis sur les projets de décisions des autorités de contrôle conformément au mécanisme de contrôle de la cohérence prévu à l'article 57, paragraphe 2, et sur les questions soumises conformément à l'article 57, paragraphe 4;

e) de promouvoir la coopération et l'échange bilatéral et multilatéral effectif d'informations et de pratiques entre les autorités de contrôle;

f) de promouvoir l'élaboration de programmes de formation conjoints et de faciliter les échanges de personnel entre autorités de contrôle, ainsi que, le cas échéant, avec les autorités de contrôle de pays tiers ou d'organisations internationales;

g) de promouvoir l'échange, avec des autorités de contrôle de la protection des données de tous pays, de connaissances et de documentation sur la législation et les pratiques en matière de protection des données;

h) (…);

i) de tenir un registre électronique accessible au public des décisions prises par les autorités de contrôle et les juridictions sur les questions traitées dans le cadre du mécanisme de contrôle de la cohérence.

2. Lorsque la Commission consulte le comité européen de la protection des données, elle peut mentionner un délai, selon l'urgence de la question.

3. Le comité européen de la protection des données transmet ses avis, lignes directrices, recommandations et bonnes pratiques à la Commission et au comité visé à l'article 87, et les publie.

Article 67

Rapports

1. (...)

2. Le comité européen de la protection des données *établit un rapport annuel sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans l'Union et,* s'il y a lieu*, dans les pays tiers* et les organisations internationales. Le rapport est publié et communiqué au Parlement européen, au Conseil et à la Commission.

3. Le rapport annuel présente notamment le bilan de l'application pratique des lignes directrices, recommandations et bonnes pratiques visées à l'article 66, paragraphe 1, point c), ainsi que des décisions contraignantes visées à l'article 57, paragraphe 3.

Article 68

Procédure

1. Le comité européen de la protection des données adopte les décisions contraignantes visées à l'article 57, paragraphe 3, conformément aux règles de majorité énoncées à l'article 58 bis, paragraphes 2 et 3. Quant aux décisions concernant les autres missions énumérées à l'article 66, elles sont prises à la majorité simple des membres du comité.

2. Le comité européen de la protection des données adopte son règlement intérieur à la majorité des deux tiers de ses membres et détermine ses modalités de fonctionnement.

Article 69

Président

1. Le comité européen de la protection des données élit son président et deux vice-présidents en son sein à la majorité simple (...) .

2. Le président et les vice-présidents sont élus pour un mandat de cinq ans renouvelable une fois.

Article 70

Missions du président

1. Le président a pour mission:

   a) de convoquer les réunions du comité européen de la protection des données et d'établir son ordre du jour;

   a *bis*) de notifier les décisions adoptées par le comité européen de la protection des données en application de l'article 58 bis à l'autorité de contrôle chef de file et aux autorités de contrôle *concernées*;

   b) de veiller à l'accomplissement, dans les délais, des missions du comité européen de la protection des données, notamment en ce qui concerne le mécanisme de contrôle de la cohérence prévu à l'article 57.

2. Le comité européen de la protection des données fixe dans son règlement intérieur la répartition des tâches entre le président et les vice-présidents.

Article 71

Secrétariat

1. Le comité européen de la protection des données dispose d'un secrétariat, qui est assuré par le secrétariat du contrôleur européen de la protection des données (...).

1 *bis*. Le secrétariat accomplit ses tâches sous l'autorité exclusive du président du comité européen de la protection des données.

1 *ter*. Pour s'acquitter de ses tâches, le personnel du secrétariat du contrôleur européen de la protection des données chargé des missions que le présent règlement confie au comité européen de la protection des données est séparé sur le plan organisationnel du personnel chargé des missions confiées au contrôleur européen de la protection des données et est soumis à des liens hiérarchiques distincts.

1 *quater*. Si nécessaire, le comité européen de la protection des données, en consultation avec le contrôleur européen de la protection des données, établit et publie un code de conduite mettant en œuvre le présent article et s'appliquant au personnel du secrétariat du contrôleur européen de la protection des données chargé des missions que le présent règlement confie au comité européen de la protection des données.

2. Le secrétariat fournit un soutien analytique, administratif et logistique au comité européen de la protection des données.

3. Le secrétariat est notamment chargé:

a) de la gestion courante du comité européen de la protection des données;

b) de la communication entre les membres du comité européen de la protection des données, son président et la Commission, et de la communication avec d'autres institutions et le public;

c) du recours à des moyens électroniques pour la communication interne et externe;

d) de la traduction des informations utiles;

e) de la préparation et du suivi des réunions du comité européen de la protection des données;

f) de la préparation, de la rédaction et de la publication d'avis, de décisions relatives au règlement des litiges entre autorités de contrôle et d'autres textes adoptés par le comité européen de la protection des données.

Article 72

Confidentialité

1. Les débats du comité européen de la protection des données sont confidentiels.

2. L'accès aux documents présentés aux membres du comité européen de la protection des données, aux experts et aux représentants de tierces parties est régi par le règlement (CE) n° 1049/2001.

CHAPITRE VIII

VOIES DE RECOURS, RESPONSABILITÉ ET SANCTIONS

Article 73

Droit d'introduire une réclamation auprès d'une autorité de contrôle

1. Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle unique, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant n'est pas conforme au présent règlement.

2. (…)

3. (…)

4. (…)

5. L'autorité de contrôle auprès de laquelle la réclamation a été introduite informe la personne à l'origine de la réclamation de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article 74 (...).

Article 74

Droit à un recours juridictionnel effectif contre une autorité de contrôle

1. Sans préjudice de tout recours administratif ou extrajudiciaire, toute personne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne.

2. Sans préjudice de tout recours administratif ou extrajudiciaire, chaque personne concernée a le droit de former un recours juridictionnel *effectif* lorsque l'autorité de contrôle compétente en vertu des articles 51 et 51 *bis* ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois ou dans un délai plus court prévu par la législation de l'Union ou d'un État membre, de l'état d'avancement ou de l'issue de sa réclamation introduite conformément à l'article 73.

3. (...) Les actions contre une (...) autorité de contrôle sont intentées devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie.

3 *bis*. Dans le cas d'une action intentée contre une décision d'une autorité de contrôle qui a été précédée d'un avis ou d'une décision du comité européen de la protection des données dans le cadre du mécanisme de contrôle de la cohérence, l'autorité de contrôle transmet l'avis ou la décision en question à la juridiction concernée.

4. (…)

5. (…)

Article 75

Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant

1. Sans préjudice de tout recours administratif ou extrajudiciaire qui leur est ouvert, notamment le droit prévu à l'article 73 de saisir une autorité de contrôle d'une réclamation, les personnes concernées disposent d'un recours juridictionnel effectif si elles considèrent qu'il a été porté atteinte aux droits que leur confère le présent règlement, à la suite du traitement de données à caractère personnel les concernant, effectué en violation du présent règlement.

2. Une action contre un responsable du traitement ou un sous-traitant est intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement (…). Une telle action peut aussi être intentée devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle, sauf si le responsable du traitement ou le sous-traitant est une autorité publique agissant dans l'exercice de ses prérogatives de puissance publique.

3. (…)

4. (…)

Article 76

Représentation des personnes concernées

1. La personne concernée a le droit de mandater un organisme, une organisation ou une association, *qui a été valablement constitué conformément au droit d'un État membre et dont les objectifs statutaires comprennent la protection des droits et des libertés des personnes concernées à l'égard de la protection de leurs données à caractère personnel, pour qu'il ou elle introduise une réclamation en son nom* et exerce en son nom les droits prévus aux articles 73, 74 et 75.

1 *bis*. (...)

2. Les États membres peuvent disposer que tout organisme, organisation ou association visé au paragraphe 1, indépendamment de tout mandat confié par une personne concernée (...), a, dans l'État membre en question, le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente conformément à l'article 73 et d'exercer les droits prévus aux articles 73, 74 et 75 s'il ou elle considère que les droits d'une personne concernée n'ont pas été respectés parce que le traitement des données à caractère personnel n'a pas eu lieu en conformité avec le présent règlement.

3. (…)

4. (…)

Article 76 bis

Suspension d'une action

1. Lorsqu'une juridiction compétente d'un État membre est informée qu'une action concernant le même objet intentée à l'égard des activités (...) du même responsable du traitement ou du même sous-traitant est pendante auprès d'une juridiction d'un autre État membre, elle contacte la juridiction en question pour confirmer l'existence d'une telle action.

2. Lorsqu'une action concernant le même objet intentée à l'égard des activités (...) du même responsable du traitement ou du même sous-traitant est pendante auprès d'une juridiction d'un autre État membre, toute juridiction compétente autre que la juridiction saisie en premier lieu peut suspendre son action.

2 *bis*. Lorsque cette action est pendante devant des juridictions du premier degré, toute juridiction autre que la juridiction saisie en premier lieu peut également se dessaisir, à la demande de l'une des parties, à condition que la juridiction première saisie soit compétente pour connaître des actions en question et que sa loi permette leur jonction.

3. (…).

Article 77

Droit à réparation et responsabilité

1. Toute personne ayant subi un dommage matériel ou immatériel du fait d'un traitement qui n'est pas conforme avec le présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

2. Tout responsable du traitement (...) ayant participé au traitement est responsable du dommage causé par le traitement qui n'est pas conforme au présent règlement. Un sous-traitant n'est tenu responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou s'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

3. Un responsable du traitement ou le sous-traitant est exonéré (...) de responsabilité, conformément au paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable (…).

4. *Si plusieurs responsables du traitement ou sous-traitants ou si un responsable du traitement et un sous-traitant participent au même traitement* et, si, *conformément aux paragraphes 2 et 3,* ils sont responsables d'un dommage causé par le traitement, (…) chacun des responsables du traitement ou des sous-traitants est (...) responsable du *dommage dans sa totalité*.

5. Lorsqu'un responsable du traitement ou un sous-traitant a, conformément au paragraphe 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées au paragraphe 2.

6. *Les actions judiciaires engagées pour exercer le droit à recevoir réparation sont intentées devant les juridictions compétentes en vertu de la législation nationale des États membres visées à l'article 75, paragraphe 2.*

Article 78

Sanctions

(…)

Article 79

Conditions générales pour l'imposition d'amendes administratives

1. Chaque autorité de contrôle (...) veille à ce que les amendes administratives visées à l'article 79 *bis* qui sont imposées en vertu du présent article pour des violations du présent règlement (...) *soient, dans chaque cas, effectives, proportionnées et dissuasives*.

2. **(…)**

2 *bis*. *Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 53, paragraphe 1 ter*, points a) à f). Lorsqu'il est décidé d'imposer ou non une amende administrative **(...)** et que le montant de l'amende administrative est fixé, il est dûment tenu compte dans chaque cas des éléments suivants:

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que *le nombre de personnes concernées en jeu et le niveau de dommage qu'elles ont subi*;

b) le fait que l'infraction a été commise de propos délibéré ou par négligence,

c) (...);

d) les mesures prises par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées;

e) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 23 et 30;

f) toute violation antérieure pertinente commise par le responsable du traitement ou le sous-traitant;

g) (…);

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant ont notifié la violation;

i) lorsque des mesures telles que celles visées à l'article 53, (…) paragraphe 1 *ter*, points a), d), e) et f), ont été précédemment décidées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, *le respect de ces mesures*;

j) l'adhésion à des codes de conduites approuvés, conformément à l'article 38, ou à des mécanismes de certification, conformément à l'article 39;

k) (…);

l) (…);

m) toute autre circonstance aggravante ou atténuante applicable au cas concerné.

3. (…)

3 *bis*. (…)

3 *ter*. Tout État membre peut établir les règles déterminant si et dans quelle mesure des amendes peuvent être infligées à des autorités et des organismes publics établis sur son territoire.

4. L'*exercice, par l'autorité de contrôle* **(…)**, des pouvoirs que lui confère le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union ou à la législation d'un État membre, y compris le droit à un recours effectif et à une procédure régulière.

5. Les États membres peuvent s'abstenir de mettre en place les règles régissant les amendes administratives visées à l'article 79 *bis*, paragraphes 1, 2 et 3, lorsque leur système juridique ne prévoit pas d'amendes administratives et que les violations visées font déjà l'objet de sanctions pénales dans le cadre de leur droit interne à la date du [date visée à l'article 91, paragraphe 2], tout en prenant les mesures nécessaires pour que ces sanctions pénales soient effectives, proportionnées et dissuasives, compte tenu du niveau des amendes administratives prévues dans le présent règlement.

Dans ce cas, les États membres notifient à la Commission les parties de leur droit pénal concernées.

Article 79 bis

Amendes administratives

1. L'autorité de contrôle (...) peut infliger une amende n'excédant pas 250 000 EUR, ou, dans le cas d'une entreprise, 0,5 % de son chiffre d'affaires annuel total au niveau mondial pour l'exercice précédent, à un responsable du traitement qui, de propos délibéré ou par négligence:

a) ne répond pas dans les délais prévus à l'article 12, paragraphe 2, aux demandes de la personne concernée;

b) perçoit des frais (…) en violation de l'article 12, paragraphe 4, première phrase.

2. L'autorité de contrôle (...) peut infliger une amende n'excédant pas 500 000 EUR ou, dans le cas d'une entreprise, 1 % de son chiffre d'affaires annuel (…) total au niveau mondial pour l'exercice précédent, à un responsable du traitement ou à un sous-traitant qui, de propos délibéré ou par négligence:

a) ne fournit pas les informations, fournit des informations incomplètes ou ne fournit pas les informations [en temps voulu ou] de façon [suffisamment] transparente à la personne concernée conformément à l'article 12, paragraphe 3, et aux articles 14 et 14 *bis*;

b) ne fournit pas un accès à la personne concernée ou ne rectifie pas les données à caractère personnel conformément aux articles 15 et 16 **(...)**;

c) n'efface pas les données à caractère personnel en violation du droit à l'effacement et à l'"oubli numérique" conformément à l'article 17, paragraphe 1, points a), b), d) ou e);

d) (…)

d *bis*) traite des données à caractère personnel en violation du droit à la limitation du traitement prévu à l'article 17 *bis* ou n'informe pas la personne concernée avant que la limitation du traitement soit levée conformément à l'article 17 *bis*, paragraphe 4;

d *ter*) ne communique pas à chaque destinataire à qui le responsable du traitement a communiqué des données à caractère personnel toute rectification, tout effacement ou toute limitation du traitement en violation de l'article 17 *ter*;

d *quater*) ne fournit pas à la personne concernée les données à caractère personnel la concernant (...) en violation de l'article 18;

d *quinquies*) traite des données à caractère personnel après que la personne concernée s'y soit opposée conformément à l'article 19, paragraphe 1, et n'établit pas l'existence de raisons impérieuses et légitimes justifiant le traitement, qui priment les intérêts, les droits et les libertés de la personne concernée, ou la constatation, l'exercice ou la défense d'un droit en justice;

d *sexies*) ne fournit pas à la personne concernée d'informations concernant le droit de s'opposer au traitement à des fins de prospection conformément à l'article 19, paragraphe 2, ou continue le traitement de données à des fins de prospection après l'opposition de la personne concernée, en violation de l'article 19, paragraphe 2 *bis*;

e) omet de définir ou ne définit pas suffisamment les obligations respectives des responsables conjoints du traitement conformément à l'article 24;

f) ne tient pas, ou pas suffisamment, à jour la documentation conformément à l'article 28 et à l'article 31, paragraphe 4.

g) (…)

3. L'autorité de contrôle (...) peut infliger une amende n'excédant pas 1 000 000 EUR ou, dans le cas d'une entreprise, 2 % de son chiffre d'affaires annuel total au niveau mondial pour l'exercice précédent, à un responsable du traitement ou à un sous-traitant qui, de propos délibéré ou par négligence:

a) traite des données à caractère personnel sans base juridique (...) à cette fin ou ne respecte pas les conditions relatives au consentement conformément aux articles 6, 7, 8 et 9;

b) (…);

c) (…);

d) ne respecte pas les conditions relatives à la prise de décision individuelle automatisée, y compris le (…) profilage conformément à l'article 20;

d *bis*) omet (…) de mettre en œuvre les mesures appropriées ou n'est pas à même d'établir le respect des obligations énoncées aux articles 22 (…) et 30;

d *ter*) omet de désigner un représentant en violation de l'article 25;

d *quater*) traite des données à caractère personnel ou donne l'instruction d'en effectuer le traitement en violation (…) de l'article 26;

d *quinquies*) omet de signaler ou de notifier une violation de données à caractère personnel, ou omet de notifier la violation [en temps utile ou] de façon complète à l'autorité de contrôle ou à la personne concernée en violation des articles 31 et 32;

d sexies) omet d'effectuer une analyse d'impact relative à la protection des données en violation de l'article 33 ou traite des données à caractère personnel sans consultation préalable de l'autorité de contrôle en violation de l'article 34, paragraphe 2;

e) (…);

f) fait un usage abusif d'une marque ou d'un label de protection des données au sens de l'article 39 ou ne respecte par les conditions et les procédures prévues aux articles 38 *bis* et 39 *bis*;

g) effectue ou donne l'instruction d'effectuer, vers un destinataire situé dans un pays tiers ou à une organisation internationale, un transfert de données en violation des articles 41 à 44;

h) ne respecte pas une injonction, une limitation temporaire ou définitive de traitement ou la suspension de flux de données par l'autorité de contrôle conformément à l'article 53, paragraphe 1 *ter*, ou ne fournit pas l'accès en violation de l'article 53, paragraphe 1.

i) (…)

j) (…).

3 *bis*. Si un responsable du traitement ou un sous-traitant enfreint délibérément ou par négligence plusieurs dispositions du présent règlement énumérées aux paragraphes 1, 2 ou 3, le montant total de l'amende ne peut pas excéder le montant fixé pour la violation la plus grave.

4. (...)

Article 79 ter

Sanctions

1. Pour les violations (...) du présent règlement, en particulier celles qui ne font pas l'objet des amendes administratives prévues à (...) *l'article 79 bis, les États membres déterminent le régime des sanctions applicables en cas de telles violations et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre (...). Ces sanctions sont effectives, proportionnées et dissuasives.*

2. (...).

3. Chaque État membre notifie à la Commission les dispositions de la législation qu'il adopte en vertu du paragraphe 1, au plus tard à la date figurant à l'article 91, paragraphe 2, et, sans délai, toute modification ultérieure les affectant.

CHAPITRE IX
DISPOSITIONS RELATIVES À DES SITUATIONS PARTICULIÈRES DE TRAITEMENT DES DONNÉES

Article 80

Traitements des données à caractère personnel et liberté d'expression <u>et d'information</u>

1. <u>La législation nationale de</u> l'État membre (…) concilie le droit à la protection des données à caractère personnel <u>prévu par le règlement</u> et le <u>droit à</u> la liberté d'expression <u>et d'information , y compris le traitement de données à caractère personnel aux fins de journalisme et aux fins d'expression universitaire, artistique ou littéraire</u>.

2. <u>*Aux fins du traitement de données à caractère personnel réalisé à des fins de journalisme ou à des fins d'expression universitaire, artistique ou littéraire,*</u> <u>les États membres prévoient des exemptions ou des dérogations aux dispositions du chapitre II (principes), du chapitre III (droits de la personne concernée), du chapitre IV (responsable du traitement et sous-traitant), du chapitre V (transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales), du chapitre VI (autorités de contrôle indépendantes) et du chapitre VII (coopération et cohérence) si celles-ci sont nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information</u> (…).

<u>Article 80 bis</u>

<u>Traitements de données à caractère personnel et accès aux documents publics</u>

<u>Les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique ou par un organisme public ou un organisme privé pour l'exécution d'une tâche réalisée dans l'intérêt public, peuvent être communiquées par ladite autorité ou ledit organisme conformément au droit de l'Union ou de l'État membre dont relève l'autorité publique ou l'organisme public, afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel prévu par le présent règlement.</u>

Article 80 bis bis

Traitement des données à caractère personnel et réutilisation des informations du secteur public

Les données à caractère personnel figurant dans des informations du secteur public détenues par une autorité publique ou par un organisme *public* ou un *organisme* privé pour l'exécution d'une tâche réalisée dans l'intérêt public, *peuvent être communiquées par ladite autorité ou ledit organisme conformément au droit de l'Union ou de l'État membre dont relève l'autorité publique ou l'organisme public*, afin de concilier la réutilisation de ces documents officiels et des informations du secteur public et *le droit à la protection des données à caractère personnel prévu par le présent règlement*.

Article 80 ter

Traitement d'un numéro d'identification national

Les États membres peuvent fixer les conditions spécifiques du traitement d'un numéro d'identification national ou de tout autre identifiant d'application générale. Dans un tel cas, le numéro d'identification national ou tout autre identifiant d'application générale n'est utilisé que dans le respect des garanties appropriées applicables aux droits et libertés de la personne concernée prévues par le présent règlement.

Article 81

Traitement de données à caractère personnel à des fins liées à la santé

(…)

Article 81 bis

Traitement de données génétiques

(…)

Article 82

Traitements de données en matière d'emploi

1. Les États membres peuvent prévoir, par voie législative ou au moyen de conventions collectives, des règles plus précises pour assurer la protection des droits et des libertés en ce qui concerne le traitement des données à caractère personnel des salariés en matière d'emploi, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.
(…)

2. Chaque État membre notifie à la Commission les dispositions de la législation qu'il adopte en vertu du paragraphe 1, au plus tard à la date figurant à l'article 91, paragraphe 2, et, sans délai, toute modification ultérieure les affectant.

3. Les États membres peuvent fixer, par voie législative, les conditions dans lesquelles les données à caractère personnel en matière d'emploi peuvent être traitées sur la base du consentement du salarié.

Article 82 bis

Traitement de données à des fins de protection sociale

(…)

Article 83

Dérogations applicables au traitement de données à caractère personnel à des fins d'archivage dans l'intérêt public ou à des fins scientifiques, statistiques et historiques

1. Lorsque les données à caractère personnel sont traitées à des fins scientifiques, statistiques ou historiques, le droit de l'Union ou de l'État membre peut, sous réserve de garanties appropriées applicables aux droits et aux libertés de la personne concernée, prévoir des dérogations à l'article 14 *bis*, paragraphes 1 et 2, et aux articles 15, 16, 17, 17 *bis*, 17 *ter*, 18 et 19, dans la mesure où de telles dérogations sont nécessaires pour atteindre les finalités concernées.

1 *bis*. Lorsque les données à caractère personnel sont traitées à des fins d'archivage dans l'intérêt public, le droit de l'Union ou de l'État membre peut, sous réserve de garanties appropriées applicables aux droits et aux libertés de la personne concernée, prévoir des dérogations à l'article 14 *bis*, paragraphes 1 et 2, aux articles 15, 16, 17, 17 *bis*, 17 *ter*, 18, 19, 23, 32 et 33 et à l'article 53, paragraphe 1, points b), d) et e), dans la mesure où de telles dérogations sont nécessaires pour atteindre les finalités concernées.

1 *ter* Dans le cas où un type de traitement visé aux paragraphes 1 et 1 *bis* sert dans le même temps une autre finalité, les dérogations autorisées sont applicables au seul traitement effectué aux fins visées auxdits paragraphes.

2. Les garanties appropriées visées aux paragraphes 1 et 1 *bis* sont énoncées dans la législation de l'Union ou de l'État membre et sont de nature à assurer que les mesures de protection technologiques et/ou organisationnelles prévues par le présent règlement sont appliquées aux données à caractère personnel (…), pour réduire au minimum le traitement des données à caractère personnel conformément aux principes de proportionnalité et de nécessité, par exemple, la *pseudonymisation des données*, à moins que ces mesures n'empêchent la réalisation de la finalité du traitement et que cette finalité ne puisse être atteinte d'une autre façon par un moyen raisonnable.

3. (…).

Article 84

Obligations de secret

1. (...) Les États membres peuvent adopter des règles spécifiques afin de définir les pouvoirs (...) des autorités de contrôle visés à l'article 53, paragraphe 1, points d *bis*) et d *ter*), en ce qui concerne les responsables du traitement ou les sous-traitants qui sont soumis, en vertu du droit de l'Union ou de l'État membre ou de réglementations arrêtées par les autorités nationales compétentes, à une obligation de secret professionnel, à d'autres obligations de secret équivalentes ou à un code de déontologie dont le contrôle et le respect des règles sont assurés par des organismes professionnels, lorsque de telles règles sont nécessaires et proportionnées pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret. Ces règles ne sont applicables qu'en ce qui concerne les données à caractère personnel que le responsable du traitement ou le sous-traitant a reçues ou s'est procurées dans le cadre d'une activité couverte par ladite obligation de secret.

2. Chaque État membre notifie à la Commission les dispositions qu'il adopte conformément au paragraphe 1, au plus tard à la date visée à l'article 91, paragraphe 2, et, sans délai, toute modification ultérieure les affectant.

Article 85

Règles existantes des églises et associations religieuses en matière de protection des données

1. Lorsque, dans un État membre, des églises et des associations ou communautés religieuses appliquent, à la date d'entrée en vigueur du présent règlement, un ensemble complet de règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, elles peuvent continuer d'appliquer lesdites règles à condition de les mettre en conformité avec les dispositions du présent règlement.

2. Les églises et les associations religieuses qui appliquent un ensemble complet de règles conformément au paragraphe 1 sont soumises au contrôle d'une autorité de contrôle indépendante qui peut être spécifique, pour autant qu'elle remplisse les conditions énoncées au chapitre VI du présent règlement.

CHAPITRE X
ACTES DÉLÉGUÉS ET ACTES D'EXÉCUTION

Article 86

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées dans le présent article.

2. La délégation de pouvoir visée à (…) l'article 39 *bis*, paragraphe 7, (…) est conférée à la Commission pour une durée indéterminée à compter de la date d'entrée en vigueur du présent règlement.

3. La délégation de pouvoir visée à (…) l'article 39 *bis*, paragraphe 7, **(…)** peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui y est précisée. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

5. Un acte délégué adopté en vertu de (…) l'article 39 *bis*, paragraphe 7, (…) n'entre en vigueur que si le Parlement européen ou le Conseil n'ont pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 87

Procédure de comité

1. La Commission est assistée par un comité. Ce comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 8 du règlement (UE) n° 182/2011, en liaison avec l'article 5, s'applique.

CHAPITRE XI

DISPOSITIONS FINALES

Article 88

Abrogation de la directive 95/46/CE

1. La directive 95/46/CE est abrogée.

2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE s'entendent comme faites au comité européen de la protection des données institué par le présent règlement.

Article 89

Relation avec la directive 2002/58/CE et modification de cette directive

1. Le présent règlement n'impose pas d'obligations supplémentaires aux personnes physiques ou morales quant au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union en ce qui concerne les domaines dans lesquels elles sont soumises à des obligations spécifiques ayant le même objet que celles énoncées dans la directive 2002/58/CE.

2 (...)

Article 89 bis

Relation avec les accords conclus antérieurement

Les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales qui ont été conclus par les États membres avant l'entrée en vigueur du présent règlement et qui sont conformes à la directive 95/46/CE restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation.

Article 90

Évaluation

1. La Commission présente périodiquement des rapports sur l'évaluation et la révision du présent règlement au Parlement européen et au Conseil.

2. Dans le cadre de ces évaluations, la Commission examine, en particulier, l'application et le fonctionnement des dispositions du chapitre VII concernant la coopération et la cohérence.

3. Le premier rapport est présenté au plus tard quatre ans après l'entrée en vigueur du présent règlement. Les rapports suivants sont ensuite présentés tous les quatre ans. Ces rapports sont publiés.

4. Pour autant que de besoin, la Commission soumet les propositions voulues pour modifier le présent règlement et pour adapter d'autres instruments juridiques, en tenant compte, notamment, de l'évolution de la technologie de l'information et des progrès de la société de l'information.

Article 91

Entrée en vigueur et application

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

2. Il est applicable à partir du [*deux ans à compter de la date visée au paragraphe 1*].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles,

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*