RÈGLEMENT (UE) 2018/1725 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 23 octobre 2018

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE

(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 ([1]),

statuant conformément à la procédure législative ordinaire ([2]),

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 (ci-après dénommée «Charte») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant. Ce droit est également garanti par l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

(2) Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil ([3]) donne aux personnes physiques des droits juridiquement protégés, définit les obligations des responsables du traitement au sein des institutions et organes communautaires en matière de traitement des données et crée une autorité de contrôle indépendante, le Contrôleur européen de la protection des données, responsable de la surveillance des traitements de données à caractère personnel effectués par les institutions et organes de l'Union. Il ne s'applique toutefois pas au traitement des données à caractère personnel dans le cadre des activités des institutions et organes de l'Union qui ne relèvent pas du droit de l'Union.

(3) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) et la directive (UE) 2016/680 du Parlement européen et du Conseil ([5]) ont été adoptés le 27 avril 2016. Alors que le règlement définit des règles générales visant à protéger les personnes physiques à l'égard du traitement des données à caractère personnel et à garantir la libre circulation de ces données dans l'Union, la directive définit les règles spécifiques visant à protéger les personnes physiques à l'égard du traitement des données à caractère personnel et à garantir la libre circulation de ces données dans l'Union dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière.

(4) Le règlement (UE) 2016/679 apporte les adaptations nécessaires au règlement (CE) n° 45/2001 en vue de garantir un cadre de protection des données solide et cohérent dans l'Union et permettre que celui-ci s'applique en parallèle avec le règlement (UE) 2016/679.

(5) Il est dans l'intérêt d'une approche cohérente de la protection des données à caractère personnel dans l'ensemble de l'Union, et de la libre circulation des données à caractère personnel au sein de l'Union, d'aligner autant que possible les règles en matière de protection des données pour les institutions, organes et organismes de l'Union sur les règles en matière de protection des données adoptées pour le secteur public dans les États membres. Chaque fois que les dispositions du présent règlement suivent les mêmes principes que les dispositions du règlement (UE) 2016/679, ces

---

([1]) JO C 288 du 31.8.2017, p. 107.

([2]) Position du Parlement européen du 13 septembre 2018 (non encore parue au Journal officiel) et décision du Conseil du 11 octobre 2018.

([3]) Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

([4]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([5]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

deux ensembles de dispositions devraient, conformément à la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée «Cour»), être interprétées de manière homogène, notamment en raison du fait que le régime du présent règlement devrait être compris comme étant équivalent au régime du règlement (UE) 2016/679.

(6) Les personnes dont les données à caractère personnel sont traitées par les institutions et organes de l'Union dans quelque contexte que ce soit, par exemple parce qu'elles sont employées par ces institutions et organes, devraient être protégées. Le présent règlement ne devrait pas s'appliquer au traitement des données à caractère personnel des personnes décédées. Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concerne les personnes morales, et en particulier les entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale.

(7) Afin d'éviter de créer un risque grave de contournement, la protection des personnes physiques devrait être neutre sur le plan technologique et ne devrait pas dépendre des techniques utilisées.

(8) Le présent règlement devrait s'appliquer au traitement des données à caractère personnel par l'ensemble des institutions, organes et organismes de l'Union. Il devrait s'appliquer au traitement des données à caractère personnel automatisé en tout ou en partie et au traitement non automatisé des données à caractère personnel contenues ou appelées à figurer 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.

(9) Dans la déclaration n° 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, annexée à l'acte final de la Conférence intergouvernementale qui a adopté le traité de Lisbonne, la conférence a reconnu que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière se basant sur l'article 16 du traité sur le fonctionnement de l'Union européenne pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines. Un chapitre distinct du présent règlement, contenant des règles générales, devrait donc s'appliquer au traitement des données opérationnelles à caractère personnel, telles que les données à caractère personnel traitées à des fins d'enquête pénale par les organes ou organismes de l'Union lorsqu'ils exercent des activités dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière.

(10) La directive (UE) 2016/680 fixe des règles harmonisées pour la protection et la libre circulation des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Afin d'assurer le même niveau de protection pour les personnes physiques à l'aide de droits opposables dans l'ensemble de l'Union et d'éviter que des divergences n'entravent les échanges de données à caractère personnel entre les organes ou organismes de l'Union lorsqu'ils exercent des activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne et les autorités compétentes, les règles pour la protection et la libre circulation des données opérationnelles à caractère personnel traitées par lesdits organes ou organismes de l'Union devraient être conformes à la directive (UE) 2016/680.

(11) Les règles générales du chapitre du présent règlement sur le traitement des données opérationnelles à caractère personnel devraient s'appliquer sans préjudice des règles spécifiques applicables au traitement des données opérationnelles à caractère personnel par les organes et organismes de l'Union lorsqu'ils exercent des activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne. Ces règles spécifiques devraient être considérées comme une lex specialis par rapport aux dispositions du chapitre du présent règlement sur le traitement des données opérationnelles à caractère personnel (lex specialis derogat legi generali). Afin de réduire la fragmentation juridique, les règles spécifiques en matière de protection des données applicables au traitement des données opérationnelles à caractère personnel par les organes ou organismes de l'Union lorsqu'ils exercent des activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne devraient être conformes aux principes qui sous-tendent le chapitre du présent règlement sur le traitement des données opérationnelles à caractère personnel, ainsi qu'aux dispositions du présent règlement relatives à un contrôle indépendant, aux voies de recours, à la responsabilité et aux sanctions.

(12) Le chapitre du présent règlement sur le traitement des données opérationnelles à caractère personnel devrait s'appliquer aux organes et organismes de l'Union lorsqu'ils exercent, que ce soit à titre principal ou accessoire, des activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. Cependant, il ne devrait s'appliquer à Europol ou au Parquet européen qu'une fois que les actes juridiques instituant Europol et le Parquet européen auront été modifiés de manière que le chapitre du présent règlement sur le traitement des données opérationnelles à caractère personnel, tel qu'adapté, leur soit applicable.

(13) La Commission devrait procéder à un réexamen du présent règlement, en particulier du chapitre du présent règlement sur le traitement des données opérationnelles à caractère personnel. La Commission devrait également procéder à un réexamen des autres actes juridiques adoptés sur la base des traités qui régissent le traitement des données opérationnelles à caractère personnel par les organes ou organismes de l'Union lorsqu'ils exercent des

activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne. Au terme de ce réexamen, pour assurer une protection uniforme et cohérente des personnes physiques à l'égard du traitement des données à caractère personnel, la Commission devrait pouvoir présenter des propositions législatives appropriées, y compris des adaptations du chapitre du présent règlement sur le traitement des données opérationnelles à caractère personnel nécessaires en vue de l'appliquer à Europol et au Parquet européen. Les adaptations devraient tenir compte des dispositions relatives à un contrôle indépendant, aux voies de recours, à la responsabilité et aux sanctions.

(14) Le traitement des données administratives à caractère personnel, telles que les données relatives au personnel, par les organes ou organismes de l'Union lorsqu'ils exercent des activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne devrait être couvert par le présent règlement.

(15) Il convient que le présent règlement s'applique au traitement des données à caractère personnel par les institutions, organes ou organismes de l'Union lorsqu'ils exercent des activités relevant du champ d'application du titre V, chapitre 2, du traité sur l'Union européenne. Le présent règlement ne devrait pas s'appliquer au traitement des données à caractère personnel par des missions visées à l'article 42, paragraphe 1, et aux articles 43 et 44 du traité sur l'Union européenne, qui mettent en œuvre la politique de sécurité et de défense commune. Le cas échéant, des propositions pertinentes devraient être présentées pour réglementer davantage le traitement des données à caractère personnel dans le domaine de la politique de sécurité et de défense commune.

(16) Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée n'est pas ou n'est plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche.

(17) 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 remplir leurs obligations en matière de protection des données. L'introduction explicite de la pseudonymisation dans le présent règlement ne vise pas à exclure toute autre mesure de protection des données.

(18) Les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion («cookies») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes.

(19) Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles. Si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel le consentement est accordé. Dans le même temps, la personne concernée devrait avoir le droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci. Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement des données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement et

qu'il est dès lors improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. Souvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Par conséquent, les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. 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.

(20) Tout traitement de données à caractère personnel devrait être licite et loyal. Le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées. Le principe de transparence exige que toute information et toute communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples. Ce principe vaut, notamment, pour les informations communiquées aux 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 physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement. Les personnes physiques devraient être informées des risques, des règles, des garanties et des droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement. En particulier, les finalités spécifiques du traitement des données à caractère personnel devraient être explicites et légitimes, et déterminées lors de la collecte des données à caractère personnel. Les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cela exige, notamment, de garantir que la durée de conservation des données est 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 à caractère personnel ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique. Il y a lieu de prendre toutes les mesures raisonnables afin de garantir que les données à caractère personnel qui sont inexactes sont rectifiées ou supprimées. Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées en ce qui les concerne, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement, l'utilisation non autorisée de ces données et de cet équipement ainsi que la divulgation non autorisée de ces données lors de leur transmission.

(21) Conformément au principe de responsabilité, lorsque des institutions et organes de l'Union transmettent des données à caractère personnel en interne et que le destinataire n'est pas un responsable du traitement ou les transmettent à d'autres institutions ou organes, ils devraient vérifier si ces données à caractère personnel sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire. En particulier, à la suite d'une demande de transmission de données à caractère personnel par le destinataire, le responsable du traitement devrait vérifier l'existence d'un motif valable justifiant le traitement licite des données à caractère personnel ainsi que la compétence du destinataire. Le responsable du traitement devrait également procéder à une évaluation provisoire de la nécessité de la transmission des données. Si des doutes se font jour quant à la nécessité de cette transmission, le responsable du traitement devrait demander au destinataire un complément d'informations. Le destinataire devrait veiller à ce que la nécessité de la transmission des données puisse être vérifiée ultérieurement.

(22) Pour être licite, le traitement de données à caractère personnel devrait être fondé sur la nécessité pour les institutions et organes de l'Union d'exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont ils sont investis, sur la nécessité de respecter une obligation légale à laquelle le responsable du traitement est soumis ou sur tout autre fondement légitime prévu par le présent règlement, y compris le consentement de la personne concernée, la nécessité d'exécuter un contrat auquel la personne concernée est partie ou pour prendre des mesures précontractuelles à la demande de la personne concernée. Le traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et organes de l'Union comprend le traitement de données à caractère personnel nécessaire pour la gestion et le fonctionnement de ces institutions et organes. 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 à celle d'une autre personne physique. Le traitement de données à caractère personnel fondé sur l'intérêt vital d'une autre personne physique ne devrait en principe avoir lieu que lorsque le traitement ne peut manifestement pas être fondé sur une autre base juridique. Certains types de traitement 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, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine.

(23) Le droit de l'Union visé dans le présent règlement devrait être clair et précis et son application devrait être prévisible pour les personnes qui y sont soumises, conformément aux exigences énoncées dans la Charte et dans la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

(24) Les règles internes visées dans le présent règlement devraient être des actes de portée générale clairs et précis destinés à produire des effets juridiques vis-à-vis des personnes concernées. Elles devraient être adoptées au niveau le plus élevé de la hiérarchie des institutions et organes de l'Union, dans la limite de leurs compétences et pour ce qui concerne des questions liées à leur fonctionnement. Elles devraient faire l'objet d'une publication au *Journal officiel de l'Union européenne*. Il convient que l'application de ces règles soit prévisible pour les personnes qui y sont soumises, conformément aux exigences énoncées dans la Charte et dans la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Les règles internes peuvent prendre la forme de décisions, en particulier lorsqu'elles sont adoptées par les institutions de l'Union.

(25) Le traitement de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement ne devrait être autorisé que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement. Dans ce cas, aucune base juridique distincte de celle qui a permis la collecte des données à caractère personnel 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 peut déterminer et préciser les missions et les finalités pour lesquelles le traitement ultérieur devrait être considéré comme compatible et licite. Le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques devrait être considéré comme une opération de traitement licite compatible. La base juridique prévue par le droit de l'Union en ce qui concerne le traitement de données à caractère personnel peut également constituer la base juridique pour un traitement ultérieur. Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres: de tout lien entre ces finalités et les finalités du traitement ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données; de la nature des données à caractère personnel; des conséquences pour les personnes concernées du traitement ultérieur prévu; et de l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu.

(26) 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 consenti à l'opération de traitement. En particulier, dans le cadre d'une déclaration écrite relative à une autre question, des garanties devraient exister afin de garantir que la personne concernée est consciente du consentement donné et de sa portée. Conformément à la directive 93/13/CEE du Conseil ([1]), une déclaration de consentement rédigée préalablement par le responsable du traitement devrait être fournie sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples, et elle ne devrait contenir aucune clause abusive. Pour que le consentement soit éclairé, la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel. Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice.

(27) Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à la création de profils de personnalité et à la collecte de données à caractère personnel relatives aux enfants lorsque des services sont proposés directement à un enfant sur des sites internet d'institutions et d'organes de l'Union, tels que des services de communication interpersonnels ou la vente en ligne de tickets, et que le traitement des données à caractère personnel repose sur le consentement.

(28) Lorsque des destinataires établis dans l'Union autres que les institutions et organes de l'Union souhaitent que des données à caractère personnel leur soient transmises par les institutions et organes de l'Union, ils devraient démontrer qu'il leur est nécessaire d'obtenir la transmission des données pour l'exécution de leur mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont ils sont investis. Une autre possibilité consisterait pour ces destinataires à démontrer qu'il est nécessaire que ces données soient transmises dans un but spécifique d'intérêt public et le responsable du traitement devrait déterminer s'il existe des raisons de penser que cette transmission pourrait porter atteinte aux intérêts légitimes de la personne concernée. En pareils cas, le responsable du traitement devrait mettre en balance, d'une manière vérifiable, les divers intérêts concurrents en vue d'évaluer la

([1]) Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs (JO L 95 du 21.4.1993, p. 29).

proportionnalité de la transmission de données à caractère personnel requise. Le but spécifique d'intérêt public pourrait avoir trait à la transparence des institutions et organes de l'Union. En outre, les institutions et organes de l'Union devraient démontrer une telle nécessité lorsqu'ils sont eux-mêmes à l'origine d'une transmission, conformément aux principes de transparence et de bonne administration. Les exigences prévues dans le présent règlement pour les transmissions à des destinataires établis dans l'Union autres que les institutions et organes de l'Union devraient s'entendre comme étant complémentaires aux conditions de licéité du traitement.

(29) Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits fondamentaux. De telles données à caractère personnel ne devraient être traitées que si les conditions spécifiques énoncées dans le présent règlement sont réunies. Ces données à caractère personnel devraient comprendre 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 adhère à des théories tendant à établir l'existence de races humaines distinctes. Le traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique. Outre les exigences spécifiques applicables au traitement des données sensibles, les principes généraux et les autres règles du présent règlement devraient s'appliquer, en particulier en ce qui concerne les conditions de licéité du traitement. Des dérogations à l'interdiction générale de traiter ces catégories particulières de données à caractère personnel devraient être explicitement prévues, entre autres lorsque la personne concernée donne son consentement explicite ou pour répondre à des besoins spécifiques, en particulier lorsque le traitement est effectué dans le cadre d'activités légitimes de certaines associations ou fondations ayant pour finalité de permettre l'exercice des libertés fondamentales.

(30) Les catégories particulières de données à caractère personnel qui méritent une protection plus élevée ne devraient être traitées à des fins liées à la santé que lorsque cela est nécessaire pour atteindre ces finalités dans l'intérêt des personnes physiques et de la société dans son ensemble, notamment dans le cadre de la gestion des services et des systèmes de soins de santé ou de protection sociale. Le présent règlement devrait dès lors 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 pour certaines fins liées à la santé par des personnes soumises à une obligation légale de secret professionnel. Le droit de l'Union devrait prévoir des mesures spécifiques et appropriées de façon à protéger les droits fondamentaux et les données à caractère personnel des personnes physiques.

(31) Le traitement des catégories particulières de données à caractère personnel peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. Un tel traitement devrait faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques. Dans ce contexte, la notion de «santé publique» devrait s'interpréter selon la définition contenue dans le règlement (CE) n° 1338/2008 du Parlement européen et du Conseil ([1]), à savoir tous les éléments relatifs à la santé, c'est-à-dire l'état de santé, morbidité et handicap inclus, les déterminants ayant un effet sur cet état de santé, les besoins en matière de soins de santé, les ressources consacrées aux soins de santé, la fourniture de soins de santé, l'accès universel à ces soins, les dépenses de santé et leur financement, ainsi que les causes de mortalité. De tels traitements de données concernant la santé pour des motifs d'intérêt public ne devraient pas aboutir à ce que des données à caractère personnel soient traitées à d'autres fins.

(32) Si les données à caractère personnel 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. L'identification devrait comprendre l'identification numérique d'une personne concernée, par exemple au moyen d'un mécanisme d'authentification tel que les mêmes identifiants, utilisé par la personne concernée pour se connecter au service en ligne proposé par le responsable du traitement.

(33) Le traitement des données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques devrait être soumis à des garanties appropriées pour les droits et libertés de la personne concernée, en vertu du présent règlement. Ces garanties devraient permettre la mise en place de mesures techniques et organisationnelles pour assurer, en particulier, le respect du principe de minimisation des données. Le traitement ultérieur de données à caractère personnel à des fins archivistiques dans l'intérêt public, à des

([1]) 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 (JO L 354 du 31.12.2008, p. 70).

fins de recherche scientifique ou historique ou à des fins statistiques doit être effectué lorsque le responsable du traitement a évalué s'il est possible d'atteindre ces finalités grâce à un traitement de données qui ne permettent pas ou plus d'identifier les personnes concernées, pour autant que des garanties appropriées existent (comme, par exemple, la pseudonymisation des données). Les institutions et organes de l'Union devraient prévoir dans le droit de l'Union des garanties appropriées pour le traitement de données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ce qui peut inclure des règles internes adoptées par les institutions et organes de l'Union pour ce qui concerne des questions liées à leur fonctionnement.

(34) Des modalités devraient être prévues pour faciliter l'exercice par la personne concernée des droits qui lui sont conférés par le présent règlement, y compris les moyens de demander et, le cas échéant, d'obtenir sans frais, notamment, l'accès aux données à caractère personnel, et leur rectification ou leur effacement, et l'exercice d'un droit d'opposition. Le responsable du traitement devrait également fournir les moyens de présenter des demandes par voie électronique, en particulier lorsque les données à caractère personnel font l'objet d'un traitement électronique. Le responsable du traitement devrait être tenu de répondre aux demandes émanant de la personne concernée dans les meilleurs délais et au plus tard dans un délai d'un mois et de motiver sa réponse lorsqu'il a l'intention de ne pas donner suite à de telles demandes.

(35) Le principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités. Le responsable du traitement devrait fournir à la personne concernée toute autre information nécessaire pour garantir un traitement équitable et transparent, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées. En outre, la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci. Lorsque les données à caractère personnel sont collectées auprès de la personne concernée, il importe que celle-ci sache également si elle est obligée de fournir ces données à caractère personnel et qu'elle soit informée des conséquences auxquelles elle s'expose si elle ne les fournit pas. Ces informations peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. Lorsque les icônes sont présentées par voie électronique, elles devraient être lisibles par machine.

(36) Les informations sur le traitement des données à caractère personnel relatives à la personne concernée devraient lui être fournies au moment où ces données sont collectées auprès d'elle ou, si les données à caractère personnel sont obtenues d'une autre source, dans un délai raisonnable en fonction des circonstances propres à chaque cas. Lorsque des données à caractère personnel peuvent être légitimement communiquées à un autre destinataire, il convient que la personne concernée soit informée du moment auquel ces données à caractère personnel sont communiquées pour la première fois audit destinataire. Lorsqu'il a l'intention de traiter les données à caractère personnel à des fins autres que celles pour lesquelles elles ont été collectées, le responsable du traitement devrait, avant de procéder à ce traitement ultérieur, fournir à la personne concernée des informations au sujet de cette autre finalité et toute autre information nécessaire. Lorsque l'origine des données à caractère personnel n'a pas pu être communiquée à la personne concernée parce que plusieurs sources ont été utilisées, des informations générales devraient être fournies.

(37) Une personne concernée devrait avoir le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet et d'exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité. Cela inclut le droit des personnes concernées d'accéder aux données concernant leur santé, par exemple les données de leurs dossiers médicaux contenant des informations telles que des diagnostics, des résultats d'examens, des avis de médecins traitants et tout traitement administré ou toute intervention pratiquée. En conséquence, toute personne concernée devrait avoir le droit de connaître et de se faire communiquer, en particulier, les finalités du traitement des données à caractère personnel, si possible la durée du traitement de ces données à caractère personnel, l'identité des destinataires de ces données à caractère personnel, la logique qui sous-tend leur éventuel traitement automatisé et les conséquences que ce traitement pourrait avoir, au moins en cas de profilage. Ce droit ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Cependant, ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée. Lorsque le responsable du traitement traite une grande quantité de données relatives à la personne concernée, il devrait pouvoir demander à celle-ci de préciser, avant de lui fournir les informations, sur quelles données ou quelles opérations de traitement sa demande porte.

(38) Les personnes concernées devraient avoir le droit de faire rectifier des données à caractère personnel les concernant, et disposer d'un «droit à l'oubli» lorsque la conservation de ces données constitue une violation du présent règlement ou du droit de l'Union auquel le responsable du traitement est soumis. Les personnes concernées devraient avoir le droit d'obtenir que leurs données à caractère personnel soient effacées et ne soient plus traitées, lorsque ces données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière, 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 ne respecte pas d'une autre manière le présent règlement. Ce droit est pertinent, en

particulier, lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente 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'est plus un enfant. Toutefois, la conservation ultérieure des données à caractère personnel 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 relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ou à la constatation, à l'exercice ou à la défense de droits en justice.

(39) Afin de renforcer le «droit à l'oubli» numérique, le droit à l'effacement devrait également être étendu de façon que le responsable du traitement qui a rendu les données à caractère personnel publiques soit tenu d'informer les responsables du traitement qui traitent ces données à caractère personnel qu'il convient d'effacer tout lien vers ces données, ou toute copie ou reproduction de celles-ci. Ce faisant, ce responsable du traitement devrait prendre des mesures raisonnables, compte tenu des technologies disponibles et des moyens dont il dispose, y compris des mesures techniques, afin d'informer les responsables du traitement qui traitent les données à caractère personnel de la demande formulée par la personne concernée.

(40) 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 à caractère personnel sélectionnées inaccessibles aux utilisateurs, ou à retirer temporairement les données publiées d'un site internet. Dans les fichiers automatisés, la limitation du traitement devrait en principe être assurée par des moyens techniques de façon que les données à caractère personnel ne fassent pas l'objet d'opérations de traitement ultérieures et ne puissent pas être modifiées. Le fait que le traitement des données à caractère personnel est limité devrait être indiqué de manière claire dans le fichier.

(41) Pour renforcer encore le contrôle qu'elles exercent sur leurs propres données, les personnes concernées devraient aussi avoir le droit, lorsque des données à caractère personnel font l'objet d'un traitement automatisé, de recevoir les données à caractère personnel les concernant, qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé, lisible par machine et interopérable, et de les transmettre à un autre responsable du traitement. Il y a lieu d'encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données. Ce droit devrait s'appliquer lorsque la personne concernée a fourni les données à caractère personnel sur la base de son consentement ou lorsque le traitement est nécessaire pour l'exécution d'un contrat. Il ne devrait dès lors pas s'appliquer lorsque le traitement des 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 ou de recevoir des données à caractère personnel la concernant ne devrait pas créer, pour les responsables du traitement, une obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles. Lorsque, dans un ensemble de données à caractère personnel, plusieurs personnes sont concernées, le droit de recevoir les données à caractère personnel devrait s'entendre sans préjudice des droits et libertés des autres personnes concernées conformément au présent règlement. De plus, ce droit ne devrait pas porter atteinte au droit de la personne concernée d'obtenir l'effacement de données à caractère personnel ni aux limitations de ce droit comme le prévoit le présent règlement et il ne devrait pas, notamment, entraîner l'effacement de données à caractère personnel relatives à la personne concernée qui ont été fournies par celle-ci pour l'exécution d'un contrat, dans la mesure où et aussi longtemps que ces données à caractère personnel sont nécessaires à l'exécution de ce contrat. Lorsque c'est techniquement possible, la personne concernée devrait avoir le droit d'obtenir que les données soient transmises directement d'un responsable du traitement à un autre.

(42) Lorsque des données à caractère personnel pourraient être traitées de manière 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, la personne concernée devrait néanmoins avoir le droit de s'opposer au traitement de toute donnée à caractère personnel en rapport avec sa situation particulière. 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.

(43) La personne concernée devrait avoir le droit de ne pas faire l'objet d'une décision, qui peut comprendre une mesure, impliquant l'évaluation de certains aspects personnels la concernant, qui est prise sur le seul fondement d'un traitement automatisé et qui produit des effets juridiques la concernant ou qui, de façon similaire, l'affecte de manière significative, tels que des pratiques de recrutement en ligne sans aucune intervention humaine. Ce type de traitement inclut le «profilage» qui consiste en toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou

centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements, dès lors qu'il produit des effets juridiques concernant la personne en question ou qu'il l'affecte de façon similaire de manière significative.

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. En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que 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. Cette mesure ne devrait pas concerner un enfant. Afin d'assurer un traitement équitable et transparent à l'égard de la personne concernée, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées, le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer les mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui entraînent des erreurs dans les données à caractère personnel soient corrigés et que le risque d'erreur soit réduit au minimum, sécuriser les données à caractère personnel d'une manière qui tienne compte des risques susceptibles de peser sur les intérêts et les droits de la personne concernée, et prévenir, entre autres, les effets discriminatoires à l'égard des personnes physiques fondées sur l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, ou l'orientation sexuelle, ou tout traitement qui se traduit 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 qu'à des conditions spécifiques.

(44) Des limitations à certains principes spécifiques ainsi qu'au droit à l'information, au droit d'accès aux données à caractère personnel, au droit de rectification ou d'effacement de ces données, au droit à la portabilité des données, au droit à la confidentialité des données de communications électroniques ainsi qu'à la communication d'une violation de données à caractère personnel à une personne concernée et à certaines obligations connexes des responsables du traitement peuvent être imposées par des actes juridiques adoptés sur la base des traités ou des règles internes adoptées par les institutions et organes de l'Union pour ce qui concerne des questions liées à leur fonctionnement, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité publique et pour la prévention des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales. Cela comprend la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, la protection de la vie humaine, particulièrement en réponse à des catastrophes d'origine naturelle ou humaine, la protection de la sécurité intérieure des institutions et organes de l'Union et d'autres objectifs d'intérêt public importants de l'Union ou d'un État membre, en particulier les objectifs de la politique étrangère et de sécurité commune de l'Union ou un intérêt économique ou financier important de l'Union ou d'un État membre, ainsi que la tenue de registres publics pour des motifs d'intérêt public général ou la protection de la personne concernée ou des droits et libertés d'autrui, y compris la protection sociale, la santé publique et les finalités humanitaires.

(45) 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 des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec le présent règlement, y compris l'efficacité des mesures. Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques.

(46) Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, 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; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur 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 convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou 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 physiques vulnérables, en particulier les enfants; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.

(47) Il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé.

(48) La protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel exige l'adoption de mesures techniques et organisationnelles appropriées pour garantir que les exigences du présent règlement sont respectées. Afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut. Ces mesures pourraient consister, entre autres, à réduire à un minimum 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 contrôler le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics.

(49) Le règlement (UE) 2016/679 prévoit que les responsables du traitement démontrent qu'ils respectent les obligations qui leur incombent par l'application de mécanismes de certification approuvés. De même, les institutions et organes de l'Union devraient être en mesure de démontrer qu'ils respectent le présent règlement par l'obtention d'une certification, conformément à l'article 42 du règlement (UE) 2016/679.

(50) La protection des droits et libertés des personnes concernées, de même que la responsabilité des responsables du traitement et des sous-traitants, exige une répartition claire des responsabilités au titre du présent règlement, y compris lorsque le responsable du traitement détermine les finalités et les moyens du traitement conjointement avec d'autres responsables du traitement, ou lorsqu'une opération de traitement est effectuée pour le compte d'un responsable du traitement.

(51) Afin que les exigences 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 activités de traitement à un sous-traitant, le responsable du traitement 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 satisfont aux exigences du présent règlement, y compris en matière de sécurité du traitement. L'application par des sous-traitants autres que les institutions et organes de l'Union d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à démontrer le respect des obligations incombant au responsable du traitement. La réalisation d'un traitement par un sous-traitant autre qu'une institution ou un organe de l'Union devrait être régie par un contrat ou, dans le cas d'une institution ou d'un organe de l'Union agissant en tant que sous-traitant, par un contrat ou un autre acte juridique établi au titre du droit de l'Union, 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, en tenant compte des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer et du risque pour les droits et libertés de la personne concernée. Le responsable du traitement et le sous-traitant devraient pouvoir choisir de recourir à un contrat particulier ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par le Contrôleur européen de la protection des données puis par la Commission. Après la réalisation du traitement pour le compte du responsable du traitement, le sous-traitant devrait, selon le choix du responsable du traitement, renvoyer ou supprimer les données à caractère personnel, à moins que le droit de l'Union ou le droit d'un État membre auquel le sous-traitant est soumis n'exige la conservation de ces données à caractère personnel.

(52) Afin de démontrer qu'ils respectent le présent règlement, les responsables du traitement devraient tenir des registres pour les activités de traitement relevant de leur responsabilité et les sous-traitants devraient tenir des registres pour les catégories d'activités de traitement relevant de leur responsabilité. Les institutions et organes de l'Union devraient être tenus de coopérer avec le Contrôleur européen de la protection des données et de mettre ces registres à la disposition de celui-ci, sur demande, pour qu'ils servent au contrôle des opérations de traitement. Pour autant que ce soit approprié compte tenu de la taille de l'institution ou de l'organe de l'Union, les institutions et organes de l'Union devraient pouvoir établir un registre central dans lequel sont consignées leurs activités de traitement. Pour des raisons de transparence, ils devraient aussi pouvoir rendre ce registre public.

(53) Afin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux

risques et à la nature des données à caractère personnel à protéger. Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels, ou un préjudice moral.

(54) Les institutions et organes de l'Union devraient garantir la confidentialité des communications électroniques comme le prévoit l'article 7 de la Charte. Les institutions et organes de l'Union devraient, en particulier, garantir la sécurité de leurs réseaux de communications électroniques. Ils devraient protéger les informations liées à l'équipement terminal des utilisateurs ayant accès à leurs sites internet et applications mobiles accessibles au public conformément à la directive 2002/58/CE du Parlement européen et du Conseil ([1]). Ils devraient également protéger les données à caractère personnel conservées dans les annuaires d'utilisateurs.

(55) Une violation de données à caractère personnel risquerait, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral. En conséquence, dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il convient qu'il notifie cette violation de données à caractère personnel au Contrôleur européen de la protection des données dans les meilleurs délais et, lorsque c'est possible, 72 heures au plus tard après en avoir pris connaissance, à moins qu'il ne puisse démontrer, conformément au principe de responsabilité, qu'il est peu probable que la violation en question engendre un risque pour les droits et libertés des personnes physiques. Si une telle notification ne peut avoir lieu dans ce délai de 72 heures, elle devrait être assortie des motifs du retard et des informations peuvent être fournies de manière échelonnée sans autre retard indu. Si ce retard est justifié, il convient de publier dès que possible les informations moins sensibles ou moins spécifiques relatives à la violation plutôt que de résoudre entièrement l'incident qui en est à l'origine avant la notification.

(56) Le responsable du traitement devrait communiquer une violation de données à caractère personnel à la personne concernée dans les meilleurs délais lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique afin qu'elle puisse prendre les précautions qui s'imposent. La communication devrait décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels. Il convient que de telles communications aux personnes concernées soient effectuées aussi rapidement qu'il est raisonnablement possible et en coopération étroite avec le Contrôleur européen de la protection des données, dans le respect des directives données par celui-ci ou par d'autres autorités compétentes, telles que les autorités répressives.

(57) Le règlement (CE) n° 45/2001 prévoit une obligation générale pour le responsable du traitement de notifier les opérations de traitement de données à caractère personnel au délégué à la protection des données. Pour autant que ce soit approprié compte tenu de la taille de l'institution ou de l'organe de l'Union, le délégué à la protection des données doit tenir un registre des opérations de traitement notifiées. Outre cette obligation générale, des procédures et des mécanismes efficaces devraient être en mis en place pour suivre les opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, du fait de leur nature, de leur étendue, de leur contexte et de leurs finalités. De telles procédures devraient également être en place, notamment, lorsqu'il s'agit de types d'opérations de traitement qui impliquent le recours à de 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. Dans de tels cas, une analyse d'impact relative à la protection des données devrait être effectuée par le responsable du traitement, préalablement au traitement, en vue d'évaluer la probabilité et la gravité particulières du risque élevé, compte tenu de la nature, de l'étendue, du contexte et des finalités du traitement et des sources du risque. Cette analyse d'impact devrait comprendre, notamment, les mesures, garanties et mécanismes envisagés pour atténuer ce risque, assurer la protection des données à caractère personnel et démontrer le respect du présent règlement.

(58) Lorsqu'il ressort d'une analyse d'impact relative à la protection des données qu'en l'absence de garanties, de mesures de sécurité et de mécanismes pour atténuer le risque, le traitement engendrerait un risque élevé pour les droits et libertés des personnes physiques et que le responsable du traitement est d'avis que le risque ne peut être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts de mise en œuvre, il y a lieu de consulter le Contrôleur européen de la protection des données avant le début des activités de traitement. Certains types de traitements, de même que l'ampleur et la fréquence des traitements, sont susceptibles d'engendrer un tel risque élevé et pourraient également causer un dommage ou porter atteinte aux droits et libertés d'une personne physique. Le Contrôleur européen de la protection des données devrait répondre à la demande de consultation dans

([1]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

un délai déterminé. Toutefois, l'absence de réaction du Contrôleur européen de la protection des données dans ce délai devrait être sans préjudice de toute intervention de sa part effectuée dans le cadre de ses missions et de ses pouvoirs prévus par le présent règlement, y compris le pouvoir d'interdire des opérations de traitement. Dans le cadre de ce processus de consultation, il devrait être possible de soumettre au Contrôleur européen de la protection des données les résultats d'une analyse d'impact relative à la protection des données réalisée en ce qui concerne le traitement en question, en particulier les mesures envisagées pour atténuer le risque pour les droits et libertés des personnes physiques.

(59) Le Contrôleur européen de la protection des données devrait être informé des mesures administratives et consulté au sujet des règles internes adoptées par les institutions et organes de l'Union pour ce qui concerne des questions liées à leur fonctionnement lorsqu'elles prévoient le traitement de données à caractère personnel, fixent des conditions aux restrictions des droits des personnes concernées ou fournissent des garanties adéquates en ce qui concerne les droits des personnes concernées, afin d'assurer la conformité du traitement visé avec le présent règlement, en particulier, en ce qui concerne l'atténuation des risques encourus par la personne concernée.

(60) Le règlement (UE) 2016/679 a institué le comité européen de la protection des données en tant qu'organe indépendant de l'Union doté de la personnalité juridique. Le comité devrait contribuer à l'application cohérente du règlement (UE) 2016/679 et de la directive (UE) 2016/680 dans l'ensemble de l'Union, notamment en conseillant la Commission. Parallèlement, le Contrôleur européen de la protection des données devrait continuer d'exercer ses fonctions de contrôle et de conseil pour toutes les institutions et tous les organes de l'Union, que ce soit de sa propre initiative ou sur demande. Afin de garantir la cohérence des règles applicables en matière de protection des données dans l'ensemble de l'Union, la Commission, lorsqu'elle prépare des propositions ou des recommandations, devrait s'efforcer de consulter le Contrôleur européen de la protection des données. La Commission devrait être tenue de procéder à une consultation après l'adoption d'actes législatifs ou pendant l'élaboration d'actes délégués et d'actes d'exécution tels que définis aux articles 289, 290 et 291 du traité sur le fonctionnement de l'Union européenne, ainsi qu'après l'adoption de recommandations et de propositions relatives à des accords conclus avec des pays tiers et des organisations internationales visés à l'article 218 du traité sur le fonctionnement de l'Union européenne, lorsque ces actes, recommandations ou propositions ont une incidence sur le droit à la protection des données à caractère personnel. Dans de tels cas, la Commission devrait être obligée de consulter le Contrôleur européen de la protection des données, sauf lorsque le règlement (UE) 2016/679 prévoit la consultation obligatoire du comité européen de la protection des données, par exemple au sujet de décisions d'adéquation ou d'actes délégués concernant les icônes normalisées et les exigences applicables aux mécanismes de certification. Lorsque l'acte en question revêt une importance particulière pour la protection des droits et libertés des personnes physiques à l'égard du traitement de leurs données à caractère personnel, la Commission devrait pouvoir, en outre, consulter le comité européen de la protection des données. Dans de tels cas, le Contrôleur européen de la protection des données devrait, en tant que membre du comité européen de la protection des données, coordonner ses travaux avec ce dernier en vue de remettre un avis conjoint. Le Contrôleur européen de la protection des données et, le cas échéant, le comité européen de la protection des données devraient fournir leurs conseils par écrit dans un délai de huit semaines. Ce délai devrait être raccourci en cas d'urgence ou dans d'autres cas jugés appropriés, par exemple lorsque la Commission élabore des actes délégués et des actes d'exécution.

(61) Conformément à l'article 75 du règlement (UE) 2016/679, le secrétariat du comité européen de la protection des données devrait être assuré par le Contrôleur européen de la protection des données.

(62) Dans l'ensemble des institutions et organes de l'Union, un délégué à la protection des données devrait veiller à l'application des dispositions du présent règlement et conseiller les responsables du traitement et les sous-traitants au sujet du respect de leurs obligations. Ce délégué devrait être une personne possédant des connaissances spécialisées dans le domaine du droit et des pratiques en matière de protection des données, qui devrait être désigné notamment en fonction des opérations de traitement de données effectuées par le responsable du traitement ou le sous-traitant et de la protection exigée pour les données à caractère personnel concernées. Ces délégués à la protection des données devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance.

(63) Lorsque des données à caractère personnel sont transférées au départ des institutions et organes de l'Union à 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 devrait être préservé. Il y a lieu d'appliquer les mêmes garanties 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 des organisations internationales ne peuvent avoir lieu que dans le plein respect du présent règlement ainsi que des libertés et droits fondamentaux inscrits dans la Charte. Un transfert ne pourrait avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions énoncées dans les dispositions du présent règlement relatives au transfert de données à caractère personnel vers des pays tiers ou des organisations internationales sont respectées par le responsable du traitement ou le sous-traitant.

(64) La Commission peut décider, en vertu de l'article 45 du règlement (UE) 2016/679 ou de l'article 36 de la directive (UE) 2016/680, qu'un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale offre un niveau adéquat de protection des données. Dans ce cas, les transferts de données à caractère personnel vers ce pays tiers ou cette organisation internationale par une institution ou un organe de l'Union peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autre autorisation.

(65) 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 un pays tiers par des garanties appropriées en faveur de la personne concernée. Ces garanties appropriées peuvent consister à recourir à des clauses types de protection des données adoptées par la Commission, à des clauses types de protection des données adoptées par le Contrôleur européen de la protection des données ou à des clauses contractuelles autorisées par le Contrôleur européen de la protection des données. Lorsque le sous-traitant n'est ni une institution ni un organe de l'Union, lesdites garanties appropriées peuvent également consister en des règles d'entreprise contraignantes, des codes de conduite et des mécanismes de certification utilisés pour les transferts internationaux en vertu du règlement (UE) 2016/679. Ces garanties devraient assurer le respect des exigences en matière de protection des données et des droits des personnes concernées d'une manière appropriée pour le traitement au sein de l'Union, y compris l'existence de droits opposables pour la personne concernée et de voies de droit effectives, ce qui comprend le droit d'engager un recours administratif ou juridictionnel effectif et d'introduire une action en réparation, dans l'Union ou dans un pays tiers. Ces garanties devraient porter, en particulier, sur le respect des principes généraux concernant le traitement des données à caractère personnel et des principes de protection des données dès la conception et par défaut. Des transferts peuvent également être effectués par des institutions et organes de l'Union vers des autorités publiques ou des organismes publics dans des pays tiers ou vers des organisations internationales exerçant des missions ou fonctions correspondantes, y compris sur la base de dispositions à intégrer dans des arrangements administratifs, tels qu'un protocole d'accord, prévoyant des droits opposables et effectifs pour les personnes concernées. L'autorisation du Contrôleur européen de la protection des données devrait être obtenue lorsque ces garanties sont prévues dans des arrangements administratifs qui ne sont pas juridiquement contraignants.

(66) La possibilité qu'ont les responsables du traitement ou les sous-traitants de recourir à des clauses types de protection des données adoptées par la Commission ou par le Contrôleur européen de la protection des données ne devrait pas les empêcher d'inclure ces clauses dans un contrat plus large, tel qu'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 le Contrôleur européen de la protection des données et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées. Les responsables du traitement et les sous-traitants devraient être encouragés à fournir des garanties supplémentaires par l'intermédiaire d'engagements contractuels qui viendraient compléter les clauses types de protection des données.

(67) Certains pays tiers adoptent des lois, des règlements et d'autres actes juridiques qui visent à réglementer directement les activités de traitement effectuées par les institutions et organes de l'Union. Il peut s'agir de décisions de juridictions ou d'autorités administratives de pays tiers qui exigent d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel, et qui ne sont pas fondées sur un accord international en vigueur entre le pays tiers demandeur et l'Union. L'application extraterritoriale de ces lois, règlements et autres actes juridiques peut être contraire au droit international et faire obstacle à la protection des personnes physiques garantie dans l'Union par le présent règlement. Les transferts ne devraient 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, entre autres, lorsque la divulgation est nécessaire pour un motif important d'intérêt public reconnu par le droit de l'Union.

(68) Il y a lieu de prévoir, dans des situations spécifiques, la possibilité de transferts dans certains cas où la personne concernée a donné son consentement explicite, lorsque le transfert est occasionnel et nécessaire dans le cadre d'un contrat ou d'une action en justice, qu'il s'agisse d'une procédure judiciaire, administrative ou extrajudiciaire, y compris de procédures devant des organismes de régulation. Il convient également de prévoir la possibilité de transferts lorsque des motifs importants d'intérêt public établis par le droit de l'Union l'exigent, ou lorsque le transfert intervient au départ d'un registre établi par la loi et destiné à être consulté par le public ou par des personnes ayant un intérêt légitime. Dans ce dernier cas, ce transfert ne devrait pas porter sur la totalité des données à caractère personnel ni sur des catégories entières de données contenues dans le registre, à moins que le droit de l'Union ne l'autorise, et, lorsque ledit registre est destiné à être consulté par des personnes ayant un intérêt légitime, le transfert ne devrait être effectué qu'à la demande de ces personnes ou lorsqu'elles doivent en être les destinataires, compte dûment tenu des intérêts et des droits fondamentaux de la personne concernée.

(69) Ces dérogations devraient s'appliquer en particulier aux transferts de données requis et nécessaires pour des motifs importants d'intérêt public, par exemple en cas d'échange international de données entre institutions et organes de l'Union et autorités de la concurrence, administrations fiscales ou douanières, autorités de surveillance financière, services chargés des questions de sécurité sociale ou relatives à la santé publique, par exemple aux fins de la recherche des contacts 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 pour 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 peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories spécifiques de données vers un pays tiers ou une organisation internationale. Tout transfert vers une organisation humanitaire internationale 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 relevant des conventions de Genève ou de respecter le droit humanitaire international applicable dans les conflits armés, pourrait être considéré comme nécessaire pour des motifs importants d'intérêt public ou parce que ce transfert est dans l'intérêt vital de la personne concernée.

(70) En tout état de cause, lorsque la Commission ne s'est pas prononcée sur le caractère adéquat du niveau de protection des données dans un pays tiers, le responsable du traitement ou le sous-traitant devrait adopter des solutions qui garantissent aux personnes concernées des droits opposables et effectifs en ce qui concerne le traitement de leurs données dans l'Union une fois que ces données ont été transférées, de façon que lesdites personnes continuent de bénéficier des droits fondamentaux et des garanties.

(71) Lorsque des données à caractère personnel franchissent les frontières extérieures de l'Union, cela peut accroître le risque que les personnes physiques ne puissent exercer leurs droits liés 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 nationales et le Contrôleur européen de la protection des données peuvent être confrontés à l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités échappant à leur compétence territoriale. Leurs efforts pour collaborer dans un contexte transfrontière peuvent également être freinés par les pouvoirs insuffisants dont ils 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. Par conséquent, une coopération plus étroite entre le Contrôleur européen de la protection des données et les autorités de contrôle nationales devrait être encouragée afin de favoriser l'échange d'informations avec leurs homologues internationaux.

(72) La mise en place, dans le règlement (CE) n° 45/2001, du Contrôleur européen de la protection des données, qui est habilité à exercer ses missions et ses pouvoirs en toute indépendance, est un élément essentiel de la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel. Le présent règlement devrait davantage renforcer et préciser son rôle et son indépendance. Il convient que le Contrôleur européen de la protection des données soit une personne offrant toutes les garanties d'indépendance et qui possède, de manière notoire, l'expérience et les compétences requises pour l'exercice des fonctions de Contrôleur européen de la protection des données, par exemple parce qu'elle fait partie ou a fait partie d'une des autorités de contrôle instituées en vertu de l'article 51 du règlement (UE) 2016/679.

(73) Afin de garantir la cohérence dans l'ensemble de l'Union en ce qui concerne l'application des règles en matière de protection des données et le contrôle de leur respect, il convient que le Contrôleur de la protection des données ait les mêmes missions et les mêmes pouvoirs effectifs que les autorités de contrôle nationales, y compris des pouvoirs d'enquête, le pouvoir d'adopter des mesures correctrices et d'infliger des sanctions, ainsi que des pouvoirs d'autorisation et des pouvoirs consultatifs, notamment en cas de réclamation introduite par des personnes physiques, et le pouvoir de porter les violations du présent règlement à l'attention de la Cour et d'ester en justice conformément au droit primaire. Ces pouvoirs devraient également inclure celui d'imposer une limitation temporaire ou définitive au traitement, y compris une interdiction. Afin d'éviter les coûts superflus ainsi que les désagréments excessifs pour les personnes concernées qui pourraient être affectées, chaque mesure prise par le Contrôleur européen de la protection des données devrait être appropriée, nécessaire et proportionnée en vue de garantir le respect du présent règlement, devrait tenir compte des circonstances de chaque cas et respecter le droit de chacun d'être entendu avant l'adoption d'une mesure le concernant. Toute mesure juridiquement contraignante prise par le Contrôleur européen de la protection des données devrait être présentée par écrit, être claire et dénuée d'ambiguïté, indiquer la date à laquelle la mesure a été prise, porter la signature du Contrôleur européen de la protection des données, exposer les motifs justifiant la mesure et mentionner le droit à un recours effectif.

(74) La compétence en matière de contrôle dont est investi le Contrôleur européen de la protection des données ne devrait pas concerner le traitement des données à caractère personnel effectué par la Cour dans l'exercice de ses fonctions juridictionnelles, afin de préserver l'indépendance de la Cour dans l'accomplissement de ses missions judiciaires, y compris lorsqu'elle prend des décisions. Pour ce type d'opérations de traitement, la Cour devrait mettre en place un contrôle indépendant, conformément à l'article 8, paragraphe 3, de la Charte, par exemple au moyen d'un mécanisme interne.

(75) Les décisions du Contrôleur européen de la protection des données ayant trait aux exceptions, garanties, autorisations et conditions relatives aux opérations de traitement de données, telles que définies dans le présent règlement, devraient être publiées dans le rapport d'activité. Indépendamment de la publication annuelle du rapport d'activité, le Contrôleur européen de la protection des données peut publier des rapports sur des sujets spécifiques.

(76) Il convient que le Contrôleur européen de la protection des données agisse dans le respect du règlement (CE) n° 1049/2001 du Parlement européen et du Conseil ([1]).

(77) Les autorités de contrôle nationales surveillent l'application du règlement (UE) 2016/679 et contribuent 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 des données à caractère personnel dans le marché intérieur. Afin de rendre plus cohérente l'application des règles en matière de protection des données applicables dans les États membres et l'application des règles en matière de protection des données applicables aux institutions et organes de l'Union, le Contrôleur européen de la protection des données devrait coopérer efficacement avec les autorités de contrôle nationales.

(78) Dans certains cas, le droit de l'Union prévoit un modèle de contrôle coordonné, partagé entre le Contrôleur européen de la protection des données et les autorités de contrôle nationales. Le Contrôleur européen de la protection des données est également l'autorité de contrôle d'Europol et à ces fins, un modèle spécifique de coopération avec les autorités de contrôle nationales a été mis en place dans le cadre d'un comité de coopération exerçant une fonction consultative. Afin d'améliorer l'efficacité de la surveillance et du contrôle de l'application des règles matérielles relatives à la protection des données, un modèle unique et cohérent de contrôle coordonné devrait être introduit dans l'Union. La Commission devrait donc, s'il y a lieu, soumettre des propositions législatives visant à modifier les actes juridiques de l'Union qui organisent un modèle de contrôle coordonné afin de les aligner sur le modèle de contrôle coordonné prévu par le présent règlement. Le comité européen de la protection des données devrait servir de forum unique pour garantir un contrôle coordonné efficace dans tous les domaines.

(79) Toute personne concernée devrait avoir le droit d'introduire une réclamation auprès du Contrôleur européen de la protection des données et disposer du droit à un recours juridictionnel effectif devant la Cour conformément aux traités si elle estime que les droits que lui confère le présent règlement sont violés ou si le Contrôleur européen de la protection des données ne donne pas à la suite de sa réclamation, la refuse ou la rejette, en tout ou en partie, ou s'il 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 au cas d'espèce. Le Contrôleur européen de la protection des données devrait informer la personne concernée de l'état d'avancement et du résultat de la réclamation dans un délai raisonnable. Si l'affaire exige de se coordonner davantage avec une autorité de contrôle nationale, des informations intermédiaires devraient être fournies à la personne concernée. Afin de faciliter l'introduction des réclamations, le Contrôleur européen de la protection des données devrait prendre des mesures telles que la mise à disposition d'un formulaire de réclamation qui peut être également rempli par voie électronique, sans que d'autres moyens de communication ne soient exclus.

(80) Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement devrait avoir le droit d'obtenir la réparation du dommage subi auprès du responsable du traitement ou du sous-traitant, sous réserve des conditions prévues par les traités.

(81) Afin de renforcer le rôle de contrôle du Contrôleur européen de la protection des données et la mise en œuvre effective du présent règlement, le Contrôleur européen de la protection des données devrait être habilité à imposer des amendes administratives en tant que sanction de dernier recours. Ces amendes devraient avoir pour objectif de sanctionner l'institution ou l'organe de l'Union — plutôt que des personnes — qui ne respecte pas le présent règlement, afin de dissuader toute violation future du présent règlement et de promouvoir une culture de la protection des données à caractère personnel au sein des institutions et organes de l'Union. Le présent règlement devrait indiquer les infractions soumises à des amendes administratives ainsi que les plafonds et critères pour fixer les amendes correspondantes. Le Contrôleur européen de la protection des données devrait déterminer le montant des amendes dans chaque cas d'espèce, en prenant en considération toutes les caractéristiques propres à chaque cas et compte dûment tenu de la nature, de la gravité et de la durée de la violation et de ses conséquences, ainsi que des mesures prises pour garantir le respect des obligations découlant du présent règlement et pour prévenir ou atténuer les conséquences de la violation. Lorsqu'il impose une amende administrative à une institution ou un organe de l'Union, le Contrôleur européen de la protection des données devrait veiller à la proportionnalité du montant de cette amende. La procédure administrative pour imposer des amendes aux institutions et organes de l'Union devrait respecter les principes généraux du droit de l'Union tels qu'ils sont interprétés par la Cour.

(82) Lorsqu'une personne concernée estime que les droits que lui confère le présent règlement sont violés, elle devrait avoir le droit de mandater un organisme, une organisation ou une association à but non lucratif, constitué conformément au droit de l'Union ou au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des données à caractère personnel, pour qu'il introduise une

([1]) Règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

réclamation en son nom auprès du Contrôleur européen de la protection des données. L'organisme, l'organisation ou l'association en question devrait également pouvoir exercer le droit à un recours juridictionnel au nom de personnes concernées ou exercer le droit d'obtenir réparation au nom de personnes concernées.

(83) Un fonctionnaire ou autre agent de l'Union qui ne respecte pas les obligations lui incombant en vertu du présent règlement devrait être passible d'une action disciplinaire ou d'une autre action, conformément aux règles et procédures prévues dans le statut des fonctionnaires de l'Union européenne et dans le régime applicable aux autres agents de l'Union, fixés par le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil ([1]) (ci-après dénommé «statut»).

(84) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([2]). Il y a lieu d'avoir recours à la procédure d'examen pour l'adoption de clauses contractuelles types entre les responsables du traitement et les sous-traitants ainsi qu'entre les sous-traitants, pour l'adoption d'une liste d'opérations de traitement qui requièrent la consultation préalable du Contrôleur européen de la protection des données par les responsables du traitement procédant à un traitement de données à caractère personnel dans le cadre de l'exécution d'une mission d'intérêt public, et pour l'adoption de clauses contractuelles types mettant en place des garanties appropriées pour les transferts internationaux.

(85) Les informations confidentielles que les autorités statistiques de l'Union et des États membres recueillent 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. Le règlement (CE) n° 223/2009 du Parlement européen et du Conseil ([3]) contient d'autres dispositions particulières relatives aux statistiques européennes couvertes par le secret.

(86) Il convient d'abroger le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE du Parlement européen, du Conseil et de la Commission ([4]). Les références faites au règlement et à la décision abrogés devraient s'entendre comme faites au présent règlement.

(87) Afin de garantir la parfaite indépendance des membres de l'autorité de contrôle indépendante, le présent règlement devrait rester sans effet sur le mandat de l'actuel Contrôleur européen de la protection des données et de l'actuel Contrôleur adjoint. Le Contrôleur adjoint actuel devrait exercer ses fonctions jusqu'à la fin de son mandat, à moins que l'une des conditions justifiant qu'il soit mis fin prématurément au mandat du Contrôleur européen de la protection des données, énoncées dans le présent règlement, ne soit remplie. Les dispositions pertinentes du présent règlement devraient s'appliquer au Contrôleur adjoint jusqu'à la fin de son mandat.

(88) Conformément au principe de proportionnalité, il est nécessaire et approprié, afin de mettre en œuvre l'objectif fondamental consistant à garantir un niveau de protection des personnes physiques équivalent en ce qui concerne le traitement des données à caractère personnel et la libre circulation des données à caractère personnel dans l'ensemble de l'Union, de définir des règles relatives au traitement des données à caractère personnel dans les institutions et organes de l'Union. Le présent règlement n'excède pas ce qui est nécessaire pour atteindre les objectifs poursuivis, conformément à l'article 5, paragraphe 4, du traité sur l'Union européenne.

(89) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, et a rendu son avis le 15 mars 2017 ([5]),

---

([1]) JO L 56 du 4.3.1968, p. 1.

([2]) 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 (JO L 55 du 28.2.2011, p. 13).

([3]) Règlement (CE) n° 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) n° 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) n° 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 (JO L 87 du 31.3.2009, p. 164).

([4]) Décision n° 1247/2002/CE du Parlement européen, du Conseil et de la Commission du 1er juillet 2002 relative au statut et aux conditions générales d'exercice des fonctions de contrôleur européen de la protection des données (JO L 183 du 12.7.2002, p. 1).

([5]) JO C 164 du 24.5.2017, p. 2.

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 par les institutions et organes de l'Union et des règles relatives à la libre circulation des données à caractère personnel entre ces institutions et organes ou vers d'autres destinataires établis dans l'Union.

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

3. Le Contrôleur européen de la protection des données contrôle l'application des dispositions du présent règlement à tous les traitements effectués par une institution ou un organe de l'Union.

Article 2

Champ d'application

1. Le présent règlement s'applique au traitement de données à caractère personnel par toutes les institutions et tous les organes de l'Union.

2. Seuls l'article 3 et le chapitre IX du présent règlement s'appliquent au traitement des données opérationnelles à caractère personnel par les organes et organismes de l'Union lorsqu'ils exercent des activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne.

3. Le présent règlement ne s'applique au traitement des données opérationnelles à caractère personnel par Europol et le Parquet européen qu'une fois que le règlement (UE) 2016/794 du Parlement européen et du Conseil ([1]) et le règlement (UE) 2017/1939 du Conseil ([2]) ont été adaptés conformément à l'article 98 du présent règlement.

4. Le présent règlement ne s'applique pas au traitement des données à caractère personnel par les missions visées à l'article 42, paragraphe 1, et aux articles 43 et 44 du traité sur l'Union européenne.

5. 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.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1) «données à caractère personnel»: toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

2) «données opérationnelles à caractère personnel»: toutes les données à caractère personnel traitées par les organes ou organismes de l'Union lorsqu'ils exercent des activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne pour réaliser les objectifs et missions fixés dans les actes juridiques portant création desdits organes ou organismes;

([1]) Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

([2]) Règlement (UE) 2017/1939 du Conseil du 12 octobre 2017 mettant en œuvre une coopération renforcée concernant la création du Parquet européen (JO L 283 du 31.10.2017, p. 1).

3) «traitement»: toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de 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, la limitation, l'effacement ou la destruction;

4) «limitation du traitement»: le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur;

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

6) «pseudonymisation»: le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

7) «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;

8) «responsable du traitement»: l'institution ou l'organe de l'Union ou la direction générale ou toute autre entité organisationnelle qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens dudit traitement sont déterminés par un acte spécifique de l'Union, le responsable du traitement ou les critères spécifiques applicables pour le désigner peuvent être prévus par le droit de l'Union;

9) «responsables du traitement autres que les institutions et organes de l'Union»: les responsables du traitement au sens de l'article 4, point 7), du règlement (UE) 2016/679 et les responsables du traitement au sens de l'article 3, point 8), de la directive (UE) 2016/680;

10) «institutions et organes de l'Union»: les institutions, organes et organismes de l'Union créés par le traité sur l'Union européenne, le traité sur le fonctionnement de l'Union européenne ou le traité Euratom, ou en vertu de ces traités;

11) «autorité compétente»: toute autorité publique d'un État membre compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

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

13) «destinataire»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement;

14) «tiers»: une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel;

15) «consentement» de la personne concernée: toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

16) «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 non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

17) «données génétiques»: les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

18) «données biométriques»: 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;

19) «données concernant la santé»: les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;

20) «service de la société de l'information»: un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil ([1]);

21) «organisation internationale»: une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord;

22) «autorité de contrôle nationale»: une autorité publique indépendante instituée par un État membre en vertu de l'article 51 du règlement (UE) 2016/679 ou de l'article 41 de la directive (UE) 2016/680;

23) «utilisateur»: toute personne physique utilisant un réseau ou un équipement terminal fonctionnant sous le contrôle d'une institution ou d'un organe de l'Union;

24) «annuaire»: un annuaire des utilisateurs accessible au public ou un annuaire interne des utilisateurs disponible dans une institution ou un organe de l'Union ou partagé entre des institutions et organes de l'Union, que ce soit sous forme imprimée ou électronique;

25) «réseau de communications électroniques»: les systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux de Terre fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise;

26) «équipement terminal»: l'équipement terminal au sens de l'article 1er, point 1), de la directive 2008/63/CE de la Commission ([2]).

CHAPITRE II

PRINCIPES GÉNÉRAUX

Article 4

Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être:

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 13, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

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

([1]) Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

([2]) Directive 2008/63/CE de la Commission du 20 juin 2008 relative à la concurrence dans les marchés des équipements terminaux de télécommunications (JO L 162 du 21.6.2008, p. 20).

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 13, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Article 5

Licéité du traitement

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

a) 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 l'institution ou l'organe de l'Union;

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

c) 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;

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

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

2. Le fondement du traitement visé au paragraphe 1, points a) et b), est inscrit dans le droit de l'Union.

Article 6

Le traitement à une autre fin compatible

Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 25, paragraphe 1, le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres:

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

b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement;

c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 10, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 11;

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

e) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

Article 7

Conditions applicables au consentement

1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.

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 effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

Article 8

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

1. Lorsque l'article 5, paragraphe 1, point d), s'applique, 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 est licite lorsque l'enfant est âgé d'au moins treize ans. Lorsque l'enfant est âgé de moins de treize ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

2. 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 à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.

3. Le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.

Article 9

Transmission de données à caractère personnel à des destinataires établis dans l'Union autres que les institutions et organes de l'Union

1. Sans préjudice des articles 4 à 6 et de l'article 10, des données à caractère personnel ne sont transmises à des destinataires établis dans l'Union autres que les institutions et organes de l'Union que si:

a) le destinataire établit que les données sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le destinataire; ou

b) le destinataire établit qu'il est nécessaire que ces données soient transmises dans un but spécifique d'intérêt public et le responsable du traitement établit, s'il existe des raisons de penser que cette transmission pourrait porter atteinte aux intérêts légitimes de la personne concernée, qu'il est proportionné de transmettre les données à caractère personnel à cette fin précise, après avoir mis en balance, d'une manière vérifiable, les divers intérêts concurrents.

2. Lorsque la transmission au titre du présent article a lieu sur l'initiative du responsable du traitement, celui-ci démontre que la transmission de données à caractère personnel est nécessaire et proportionnée à ses finalités, en appliquant les critères énoncés au paragraphe 1, point a) ou b).

3. Les institutions et organes de l'Union concilient le droit à la protection des données à caractère personnel avec le droit d'accès aux documents conformément au droit de l'Union.

Article 10

Traitement portant sur des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique 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 pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union 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 sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée;

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 ses activités légitimes et moyennant les garanties appropriées, par un organisme à but non lucratif constituant une entité intégrée dans une institution ou un organe de l'Union 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 celui-ci des contacts réguliers en liaison avec ses finalités et que les données ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées;

e) le traitement porte sur des données à caractère personnel qui sont 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 la Cour agit dans le cadre de ses fonctions juridictionnelles;

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts 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 la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières 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 qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel; ou

j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, sur la base du droit de l'Union qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

3. Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union ou au droit d'un État membre, ou aux règles arrêtées par les organismes nationaux compétents, ou sous la responsabilité d'un tel professionnel, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre, ou aux règles arrêtées par les organismes nationaux compétents.

Article 11

Traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions

Le traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 5, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique ou si le traitement est autorisé par le droit de l'Union qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées.

Article 12

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, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le présent règlement.

2. Lorsque, dans les cas visés au paragraphe 1 du présent article, le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il en informe la personne concernée, si possible. En pareils cas, les articles 17 à 22 ne sont pas applicables, sauf lorsque la personne concernée fournit, aux fins d'exercer les droits que lui confèrent ces articles, des informations complémentaires qui permettent de l'identifier.

Article 13

Garanties applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

Le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est soumis, conformément au présent règlement, à des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties garantissent la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière.

CHAPITRE III

DROITS DE LA PERSONNE CONCERNÉE

SECTION 1

Transparence et modalités

Article 14

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 15 et 16 ainsi que pour procéder à toute communication au titre des articles 17 à 24 et de l'article 35 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens, y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

2. Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée au titre des articles 17 à 24. Dans les cas visés à l'article 12, 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 17 à 24, à moins que le responsable du traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée.

3. Le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 17 à 24, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande. Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique lorsque cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement.

4. Si le responsable du traitement ne donne pas à la suite de 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 du Contrôleur européen de la protection des données et de former un recours juridictionnel.

5. Aucun paiement n'est exigé pour fournir les informations au titre des articles 15 et 16 et pour procéder à une communication et prendre une mesure au titre des articles 17 à 24 et de l'article 35. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut refuser de donner suite à la demande. Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

6. Sans préjudice de l'article 12, lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée aux articles 17 à 23, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

7. Les informations à communiquer aux personnes concernées en application des articles 15 et 16 peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. Lorsque les icônes sont présentées par voie électronique, elles sont lisibles par machine.

8. Lorsque la Commission adopte des actes délégués en vertu de l'article 12, paragraphe 8, du règlement (UE) 2016/679 aux fins de déterminer les informations à présenter sous la forme d'icônes ainsi que les procédures régissant la fourniture d'icônes normalisées, les institutions et organes de l'Union fournissent, le cas échéant, les informations requises en vertu des articles 15 et 16 du présent règlement en combinaison avec ces icônes normalisées.

SECTION 2

Informations et accès aux données à caractère personnel

Article 15

Informations à fournir lorsque des données à caractère personnel 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 lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes:

a) l'identité et les coordonnées du responsable du traitement;

b) les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel;

e) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 48, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

2. 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 informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent:

a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou, le cas échéant, du droit de s'opposer au traitement ou du droit à la portabilité des données;

c) lorsque le traitement est fondé sur l'article 5, paragraphe 1, point d), ou sur l'article 10, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci;

d) le droit d'introduire une réclamation auprès du Contrôleur européen de la protection des données;

e) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences possibles de la non-fourniture de ces données;

f) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 24, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

3. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle elles ont été collectées, 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, 2 et 3 ne s'appliquent pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations.

Article 16

Informations à fournir lorsque les données à caractère personnel 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 fournit à celle-ci toutes les informations suivantes:

a) l'identité et les coordonnées du responsable du traitement;

b) les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) les catégories de données à caractère personnel concernées;

e) le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel;

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 48, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée les informations complémentaires suivantes nécessaires pour garantir un traitement équitable et transparent à l'égard de la personne concernée:

a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou, le cas échéant, du droit de s'opposer au traitement ou du droit à la portabilité des données;

c) lorsque le traitement est fondé sur l'article 5, paragraphe 1, point d), ou sur l'article 10, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci;

d) le droit d'introduire une réclamation auprès du Contrôleur européen de la protection des données;

e) la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant si elles sont issues ou non de sources accessibles au public;

f) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 24, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles 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 après avoir obtenu les données à caractère personnel, mais ne dépassant toutefois pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées;

b) si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne; ou

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

4. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel 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.

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

a) la personne concernée dispose déjà de ces informations;

b) la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ou dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement;

c) l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée; ou

d) les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union, y compris une obligation légale de secret professionnel.

6. Dans les cas visés au paragraphe 5, point b), le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.

Article 17

Droit d'accès de la personne concernée

1. La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que les informations suivantes:

a) les finalités du traitement;

b) les catégories de données à caractère personnel concernées;

c) les destinataires ou 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 de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

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

f) le droit d'introduire une réclamation auprès du Contrôleur européen de la protection des données;

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

h) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 24, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

2. Lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées, fournies en vertu de l'article 48, en ce qui concerne ce transfert.

3. Le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement.

4. Le droit d'obtenir une copie visé au paragraphe 3 ne porte pas atteinte aux droits et libertés d'autrui.

SECTION 3

Rectification et effacement

Article 18

Droit de rectification

La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

Article 19

Droit à l'effacement («droit à l'oubli»)

1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant, et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique:

a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;

b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 5, paragraphe 1, point d), ou à l'article 10, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement;

c) la personne concernée s'oppose au traitement en vertu de l'article 23, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement;

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

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

f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1.

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

3. Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire:

a) à l'exercice du droit à la liberté d'expression et d'information;

b) pour respecter une obligation légale 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 10, paragraphe 2, points h) et i), ainsi qu'à l'article 10, paragraphe 3;

d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou

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

Article 20

Droit à la limitation du traitement

1. La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique:

a) l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude, y compris l'exhaustivité, des données à caractère personnel;

b) le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation;

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

d) la personne concernée s'est opposée au traitement en vertu de l'article 23, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

2. Lorsque le traitement a été limité en vertu du paragraphe 1, ces données à caractère personnel 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 physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre.

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

4. En ce qui concerne les fichiers automatisés, la limitation du traitement est en principe assurée par des moyens techniques. Le fait que les données à caractère personnel font l'objet d'une limitation est indiqué dans le fichier de façon à ce qu'il apparaisse clairement que les données à caractère personnel ne peuvent pas être utilisées.

Article 21

Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement

Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectués conformément à l'article 18, à l'article 19, paragraphe 1, et à l'article 20, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.

Article 22

Droit à la portabilité des données

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

a) le traitement est fondé sur le consentement en application de l'article 5, paragraphe 1, point d), ou de l'article 10, paragraphe 2, point a), ou sur un contrat en application de l'article 5, paragraphe 1, point c); et

b) le traitement est effectué à l'aide de procédés automatisés.

2. Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre ou à des responsables du traitement autres que les institutions et organes de l'Union, lorsque cela est techniquement possible.

3. L'exercice du droit prévu au paragraphe 1 du présent article s'entend sans préjudice de l'article 19. Ce droit 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.

4. Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés d'autrui.

SECTION 4

Droit d'opposition et prise de décision individuelle automatisée

Article 23

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 un traitement des données à caractère personnel la concernant fondé sur l'article 5, paragraphe 1, point a), y compris un profilage fondé sur cette disposition. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

2. Au plus tard au moment de la première communication avec la personne concernée, le droit visé au paragraphe 1 est explicitement porté à l'attention de la personne concernée et est présenté clairement et séparément de toute autre information.

3. Sans préjudice des articles 36 et 37, dans le cadre de l'utilisation de services de la société de l'information, la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.

4. Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public.

Article 24

Décision individuelle automatisée, y compris le profilage

1. La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

2. 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 le responsable du traitement;

b) est autorisée par le droit de l'Union, qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée; ou

c) est fondée sur le consentement explicite de la personne concernée.

3. Dans les cas visés au paragraphe 2, points a) et c), le responsable du traitement met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

4. Les décisions visées au paragraphe 2 du présent article ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'article 10, paragraphe 1, à moins que l'article 10, paragraphe 2, point a) ou g), ne s'applique et que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place.

SECTION 5

Limitations

Article 25

Limitations

1. Des actes juridiques adoptés sur la base des traités ou, pour les questions concernant le fonctionnement des institutions et organes de l'Union, des règles internes fixées par ces derniers peuvent limiter l'application des articles 14 à 22, 35 et 36, ainsi que de l'article 4 dans la mesure où ses dispositions correspondent aux droits et obligations prévus aux articles 14 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir:

a) la sécurité nationale, la sécurité publique ou la défense des États membres;

b) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

c) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, en particulier les objectifs de la politique étrangère et de sécurité commune de l'Union ou 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;

d) la sécurité interne des institutions et organes de l'Union, notamment de leurs réseaux de communications électroniques;

e) la protection de l'indépendance de la justice et des procédures judiciaires;

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

g) 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) à c);

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

i) l'exécution des demandes de droit civil.

2. En particulier, les actes juridiques ou règles internes visés au paragraphe 1 contiennent des dispositions spécifiques, le cas échéant, en ce qui concerne:

a) les finalités du traitement ou des catégories de traitement;

b) les catégories de données à caractère personnel;

c) l'étendue des limitations introduites;

d) les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites;

e) la détermination du responsable du traitement ou des catégories de responsables du traitement;

f) la durée de conservation et les garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement; et

g) les risques pour les droits et libertés des personnes concernées.

3. Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, le droit de l'Union, qui peut inclure des règles internes adoptées par les institutions et organes de l'Union pour ce qui concerne des questions liées à leur fonctionnement, peut prévoir des dérogations aux droits visés aux articles 17, 18, 20 et 23, sous réserve des conditions et des garanties visées à l'article 13, dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités.

4. Lorsque des données à caractère personnel sont traitées à des fins archivistiques dans l'intérêt public, le droit de l'Union, qui peut inclure des règles internes adoptées par les institutions et organes de l'Union pour ce qui concerne des questions liées à leur fonctionnement, peut prévoir des dérogations aux droits visés aux articles 17, 18, 20, 21, 22 et 23, sous réserve des conditions et des garanties visées à l'article 13, dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités.

5. Les règles internes visées aux paragraphes 1, 3 et 4 sont des actes de portée générale, clairs et précis, destinés à produire des effets juridiques vis-à-vis des personnes concernées; elles sont adoptées au niveau le plus élevé de la hiérarchie des institutions et organes de l'Union et font l'objet d'une publication au *Journal officiel de l'Union européenne*.

6. Si une limitation est imposée en vertu du paragraphe 1, la personne concernée est informée, conformément au droit de l'Union, des principales raisons qui motivent cette limitation et de son droit de saisir le Contrôleur européen de la protection des données.

7. Si une limitation imposée en vertu du paragraphe 1 est invoquée pour refuser l'accès à la personne concernée, le Contrôleur européen de la protection des données lui fait uniquement savoir, lorsqu'il examine la réclamation, si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées.

8. La communication des informations visées aux paragraphes 6 et 7 du présent article et à l'article 45, paragraphe 2, peut être différée, omise ou refusée si elle prive d'effet la limitation imposée en vertu du paragraphe 1 du présent article.

CHAPITRE IV

RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT

SECTION 1

Obligations générales

Article 26

Responsabilité du responsable du traitement

1. Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.

2. Lorsque cela est proportionné au regard des activités de traitement, 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.

3. L'application de mécanismes de certification approuvés comme le prévoit l'article 42 du règlement (UE) 2016/679 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

Article 27

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

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective, et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles 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 à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

3. Un mécanisme de certification approuvé comme le prévoit l'article 42 du règlement (UE) 2016/679 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

Article 28

Responsables conjoints du traitement

1. Lorsque deux ou plusieurs responsables du traitement ou un ou plusieurs responsables du traitement avec un ou plusieurs responsables du traitement autres que les institutions et organes de l'Union déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs responsabilités respectives aux fins d'assurer le respect des obligations qui leur incombent en matière de protection des données, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations énumérées aux articles 15 et 16, par voie d'accord entre eux, sauf si, et dans la mesure où, leurs responsabilités respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables conjoints du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

3. 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 de et contre chacun des responsables du traitement.

Article 29

Sous-traitant

1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

2. Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe 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.

3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit 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, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant:

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;

c) prend toutes les mesures requises en vertu de l'article 33;

d) respecte les conditions énumérées aux paragraphes 2 et 4 pour recruter un autre sous-traitant;

e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de 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 33 à 41, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant;

g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel; et

h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

En ce qui concerne le premier alinéa, point h), le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

4. Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément au paragraphe 3 sont imposées 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 d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences 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.

5. Lorsqu'un sous-traitant n'est pas une institution ou un organe de l'Union, le fait qu'il applique un code de conduite approuvé, comme le prévoit l'article 40, paragraphe 5, du règlement (UE) 2016/679, ou un mécanisme de certification approuvé, comme le prévoit l'article 42 du même règlement, peut servir d'élément pour démontrer l'existence des garanties suffisantes conformément aux paragraphes 1 et 4 du présent article.

6. 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 3 et 4 du présent article peut être fondé, en tout ou en partie, sur les clauses contractuelles types visées aux paragraphes 7 et 8 du présent article, y compris lorsqu'elles font partie d'une certification délivrée au responsable du traitement autre qu'une institution ou un organe de l'Union en vertu de l'article 42 du règlement (UE) 2016/679.

7. La Commission peut établir des clauses contractuelles types pour les questions visées aux paragraphes 3 et 4 du présent article et conformément à la procédure d'examen visée à l'article 96, paragraphe 2.

8. Le Contrôleur européen de la protection des données peut adopter des clauses contractuelles types pour les questions visées aux paragraphes 3 et 4.

9. Le contrat ou l'autre acte juridique visé aux paragraphes 3 et 4 se présente sous forme écrite, y compris sous forme électronique.

10. Sans préjudice des articles 65 et 66, si, en violation du présent règlement, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement.

Article 30

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

Le sous-traitant et 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 peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligés par le droit de l'Union ou le droit d'un État membre.

Article 31

Registre des activités de traitement

1. Chaque responsable du traitement tient un registre des activités de traitement effectuées sous sa responsabilité. Ce registre comporte toutes les informations suivantes:

a) le nom et les coordonnées du responsable du traitement, du délégué à la protection des données et, le cas échéant, du sous-traitant et du responsable conjoint du traitement;

b) les finalités du traitement;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans les États membres, dans des pays tiers ou des organisations internationales;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées;

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

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 33.

2. Chaque sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant:

a) le nom et les coordonnées du ou des sous-traitants, de chaque responsable du traitement pour le compte duquel le sous-traitant agit et du délégué à la protection des données;

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

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 33.

3. Les registres visés aux paragraphes 1 et 2 se présentent sous forme écrite, y compris sous forme électronique.

4. Les institutions et organes de l'Union mettent le registre à la disposition du Contrôleur européen de la protection des données sur demande.

5. Pour autant que ce soit approprié compte tenu de la taille de l'institution ou de l'organe de l'Union, les institutions et organes de l'Union consignent leurs activités de traitement dans un registre central. Ils mettent ce registre à la disposition du public.

Article 32

Coopération avec le Contrôleur européen de la protection des données

Les institutions et organes de l'Union coopèrent avec le Contrôleur européen de la protection des données, à la demande de celui-ci, dans l'exécution de ses missions.

SECTION 2

Sécurité des données à caractère personnel

Article 33

Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, 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 afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment, de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant qui a accès à des données à caractère personnel ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union.

4. L'application d'un mécanisme de certification approuvé comme le prévoit l'article 42 du règlement (UE) 2016/679 peut servir d'élément pour démontrer le respect des exigences énoncées au paragraphe 1 du présent article.

Article 34

Notification au Contrôleur européen de la protection des données d'une violation de données à caractère personnel

1. En cas de violation de données à caractère personnel, le responsable du traitement notifie la violation en question au Contrôleur européen de la protection des données dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification au Contrôleur européen de la protection des données n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais 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, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

b) indiquer le nom et les coordonnées du délégué à la protection des données;

c) décrire les conséquences probables de la violation de données à caractère personnel;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

5. Le responsable du traitement informe le délégué à la protection des données de la violation de données à caractère personnel.

6. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation de données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet au Contrôleur européen de la protection des données de vérifier le respect du présent article.

Article 35

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

1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 34, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par la violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

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

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, le Contrôleur européen de la protection des données peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions énumérées au paragraphe 3 est remplie.

SECTION 3

Confidentialité des communications électroniques

Article 36

Confidentialité des communications électroniques

Les institutions et organes de l'Union garantissent la confidentialité des communications électroniques, en particulier en sécurisant leurs réseaux de communications électroniques.

Article 37

Protection des informations transmises ou liées à l'équipement terminal des utilisateurs et des informations qui y sont stockées, traitées ou collectées

Les institutions et organes de l'Union protègent les informations transmises ou liées à l'équipement terminal des utilisateurs ayant accès à leurs sites internet et applications mobiles accessibles au public, ou qui y sont stockées, traitées ou collectées, conformément à l'article 5, paragraphe 3, de la directive 2002/58/CE.

Article 38

Annuaires d'utilisateurs

1. Les données à caractère personnel contenues dans des annuaires d'utilisateurs et l'accès à ces annuaires sont limités à ce qui est strictement nécessaire aux fins spécifiques de l'annuaire.

2. Les institutions et organes de l'Union prennent toutes les mesures nécessaires pour empêcher que les données à caractère personnel contenues dans ces annuaires, qu'ils soient ou non accessibles au public, ne soient utilisées à des fins de prospection directe.

SECTION 4

Analyse d'impact relative à la protection des données et consultation préalable

Article 39

Analyse d'impact relative à la protection des données

1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

2. 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.

3. 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 approfondie d'aspects personnels concernant des personnes physiques qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

b) le traitement à grande échelle de catégories particulières de données visées à l'article 10, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 11; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

4. Le Contrôleur européen de la protection des données établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise en vertu du paragraphe 1.

5. Le Contrôleur européen de la protection des données peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

6. Avant d'adopter les listes visées aux paragraphes 4 et 5 du présent article, le Contrôleur européen de la protection des données demande au comité européen de la protection des données institué par l'article 68 du règlement (UE) 2016/679 d'examiner lesdites listes conformément à l'article 70, paragraphe 1, point e), dudit règlement, lorsqu'elles ont trait à des opérations de traitement effectuées par un responsable du traitement agissant conjointement avec un ou plusieurs responsables du traitement autres que les institutions et organes de l'Union.

7. L'analyse contient au moins:

a) une description systématique des opérations de traitement envisagées et des finalités du traitement;

b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;

c) une évaluation des risques pour les droits et libertés des personnes concernées visés au paragraphe 1; et

d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

8. Le respect, par les sous-traitants concernés autres que des institutions ou organes de l'Union, de codes de conduite approuvés comme prévu à l'article 40 du règlement (UE) 2016/679 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

9. Le cas échéant, 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 de la sécurité des opérations de traitement.

10. Lorsque le traitement effectué en application de l'article 5, paragraphe 1, point a) ou b), a comme base juridique un acte juridique adopté en vertu des traités, que cette base réglemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée préalablement à l'adoption de l'acte juridique en question, les paragraphes 1 à 6 du présent article ne s'appliquent pas, à moins que le droit de l'Union n'en dispose autrement.

11. Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

Article 40

Consultation préalable

1. Le responsable du traitement consulte le Contrôleur européen de la protection des données préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 39 indique qu'en l'absence de garanties, de mesures de sécurité et de mécanismes pour atténuer le risque, le traitement engendrerait un risque élevé pour les droits et libertés de personnes physiques et que le responsable du traitement est d'avis que ce risque ne peut être atténué par des moyens raisonnables, compte tenu des techniques disponibles et des coûts de mise en œuvre. Le responsable du traitement demande conseil au délégué à la protection des données quant à la nécessité d'une consultation préalable.

2. Lorsque le Contrôleur européen de la protection des données est d'avis que le traitement envisagé visé au paragraphe 1 constituerait une violation du présent règlement, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, le Contrôleur européen de la protection des données fournit par écrit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage des pouvoirs visés à l'article 58. Ce délai peut être prolongé de six semaines, en fonction de la complexité du traitement envisagé. Le Contrôleur européen de la protection des données informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard, dans un délai d'un mois à compter de la réception de la demande de consultation. Ces délais peuvent être suspendus jusqu'à ce que le Contrôleur européen de la protection des données ait obtenu les informations qu'il a demandées pour les besoins de la consultation.

3. Lorsque le responsable du traitement consulte le Contrôleur européen de la protection des données en application du paragraphe 1, il lui communique:

a) le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement;

b) les finalités et les moyens du traitement envisagé;

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

d) les coordonnées du délégué à la protection des données;

e) l'analyse d'impact relative à la protection des données prévue à l'article 39; et

f) toute autre information que le Contrôleur européen de la protection des données demande.

4. La Commission peut, par la voie d'un acte d'exécution, arrêter une liste de cas dans lesquels les responsables du traitement consultent le Contrôleur européen de la protection des données et obtiennent son autorisation préalable en ce qui concerne un traitement de données à caractère personnel effectué dans le cadre d'une mission d'intérêt public exercée par un responsable du traitement, y compris le traitement de telles données dans le cadre de la protection sociale et de la santé publique.

SECTION 5

Information et consultation législative

Article 41

Information et consultation

1. Les institutions et organes de l'Union informent le Contrôleur européen de la protection des données lorsqu'ils élaborent des mesures administratives et des règles internes relatives au traitement de données à caractère personnel par une institution ou un organe de l'Union, que ce soit seuls ou conjointement avec d'autres.

2. Les institutions et organes de l'Union consultent le Contrôleur européen de la protection des données lorsqu'ils élaborent les règles internes visées à l'article 25.

Article 42

Consultation législative

1. À la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le Contrôleur européen de la protection des données en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel.

2. Lorsqu'un acte visé au paragraphe 1 revêt une importance particulière pour la protection des droits et libertés des personnes physiques à l'égard du traitement de données à caractère personnel, la Commission peut également consulter le comité européen de la protection des données. Dans ce cas, le Contrôleur européen de la protection des données et le comité européen de la protection des données coordonnent leurs travaux en vue de formuler un avis conjoint.

3. Les avis visés aux paragraphes 1 et 2 sont communiqués par écrit dans un délai maximal de huit semaines à compter de la réception de la demande de consultation prévue aux paragraphes 1 et 2. En cas d'urgence ou s'il y a autrement lieu, la Commission peut réduire ce délai.

4. Le présent article ne s'applique pas lorsque le règlement (UE) 2016/679 fait obligation à la Commission de consulter le comité européen de la protection des données.

SECTION 6

Délégué à la protection des données

Article 43

Désignation du délégué à la protection des données

1. Chaque institution ou organe de l'Union désigne un délégué à la protection des données.

2. Un seul et même délégué à la protection des données peut être désigné pour plusieurs institutions et organes de l'Union, compte tenu de leur structure organisationnelle et de leur taille.

3. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 45.

4. Le délégué à la protection des données est un membre du personnel de l'institution ou de l'organe de l'Union. Compte tenu de leur taille et si l'option prévue au paragraphe 2 n'est pas exercée, les institutions et organes de l'Union peuvent désigner un délégué à la protection des données, qui exerce ses missions sur la base d'un contrat de service.

5. Les institutions et organes de l'Union publient les coordonnées du délégué à la protection des données et les communiquent au Contrôleur européen de la protection des données.

Article 44

Fonction du délégué à la protection des données

1. Les institutions et organes de l'Union 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. Les institutions et organes de l'Union aident le délégué à la protection des données à exercer les missions visées à l'article 45 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et en lui permettant d'entretenir ses connaissances spécialisées.

3. Les institutions et organes de l'Union veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice de ces missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

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

5. Le délégué à la protection des données et son personnel sont soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de leurs missions, conformément au droit de l'Union.

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

7. Le délégué à la protection des données peut être consulté, sans passer par les voies officielles, par le responsable du traitement et le sous-traitant, par le comité du personnel concerné ou encore par toute personne physique sur toute question concernant l'interprétation ou l'application du présent règlement. Aucune personne ne doit subir de préjudice pour avoir porté à l'attention du délégué à la protection des données compétent un fait dont elle allègue qu'il constitue une violation des dispositions du présent règlement.

8. Le délégué à la protection des données est désigné pour une période de trois à cinq ans et son mandat est renouvelable. Il ne peut être relevé de ses fonctions par l'institution ou l'organe de l'Union qui l'a désigné s'il ne remplit plus les conditions requises pour l'exercice de ses fonctions qu'avec le consentement du Contrôleur européen de la protection des données.

9. Après la désignation du délégué à la protection des données, le nom de ce dernier est communiqué au Contrôleur européen de la protection des données par l'institution ou l'organe de l'Union qui l'a désigné.

Article 45

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 employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union en matière de protection des données;

b) assurer, d'une manière indépendante, l'application interne du présent règlement; contrôler le respect du présent règlement, d'autres textes législatifs de l'Union applicables contenant des dispositions en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;

c) veiller à ce que les personnes concernées soient informées de leurs droits et obligations au titre du présent règlement;

d) dispenser des conseils, sur demande, en ce qui concerne la nécessité d'une notification ou d'une communication d'une violation de données à caractère personnel conformément aux articles 34 et 35;

e) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 39 et consulter le Contrôleur européen de la protection des données en cas de doute quant à la nécessité d'effectuer une analyse d'impact relative à la protection des données;

f) dispenser des conseils, sur demande, en ce qui concerne la nécessité d'une consultation préalable du Contrôleur européen de la protection des données en vertu de l'article 40; consulter le Contrôleur européen de la protection des données en cas de doute quant à la nécessité de le consulter préalablement;

g) répondre aux demandes du Contrôleur européen de la protection des données et, dans son domaine de compétence, coopérer et se concerter avec le Contrôleur européen de la protection des données à la demande de ce dernier ou de sa propre initiative.

h) veiller à ce que les opérations de traitement ne portent pas atteinte aux droits et libertés des personnes concernées.

2. Le délégué à la protection des données peut faire des recommandations visant à améliorer concrètement la protection des données au responsable du traitement et au sous-traitant et conseiller ces derniers sur des questions touchant à l'application des dispositions relatives à la protection des données. En outre, de sa propre initiative ou à la demande du responsable du traitement ou du sous-traitant, du comité du personnel concerné ou de toute personne physique, il peut examiner des questions et des faits qui sont directement en rapport avec ses missions et qui ont été portés à sa connaissance, et faire rapport à la personne qui a demandé cet examen ou au responsable du traitement ou au sous-traitant.

3. Des dispositions d'application complémentaires concernant le délégué à la protection des données sont adoptées par chaque institution ou organe de l'Union. Elles concernent en particulier les missions, les fonctions et les compétences du délégué à la protection des données.

CHAPITRE V

TRANSFERTS DE DONNÉES À CARACTÈRE PERSONNEL VERS DES PAYS TIERS OU À DES ORGANISATIONS INTERNATIONALES

Article 46

Principe général applicable aux transferts

Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis.

Article 47

Transferts fondés sur une décision d'adéquation

1. Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a décidé, en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 ou de l'article 36, paragraphe 3, de la directive (UE) 2016/680, 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 et que le transfert de données à caractère personnel a lieu exclusivement pour permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement.

2. Les institutions et organes de l'Union informent la Commission et le Contrôleur européen de la protection des données des cas dans lesquels ils estiment qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale en question n'assure pas un niveau de protection adéquat au sens du paragraphe 1.

3. Les institutions et organes de l'Union prennent les mesures nécessaires pour se conformer aux décisions prises par la Commission lorsque cette dernière constate, en vertu de l'article 45, paragraphe 3 ou 5, du règlement (UE) 2016/679 ou de l'article 36, paragraphe 3 ou 5, de la directive (UE) 2016/680, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale assure ou n'assure plus un niveau de protection adéquat.

Article 48

Transferts moyennant des garanties appropriées

1. En l'absence de décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 ou de l'article 36, paragraphe 3, de la directive (UE) 2016/680, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

2. Les garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela ne nécessite une autorisation particulière du Contrôleur européen de la protection des données, par:

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

b) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 96, paragraphe 2;

c) des clauses types de protection des données adoptées par le Contrôleur européen de la protection des données et approuvées par la Commission en conformité avec la procédure d'examen visée à l'article 96, paragraphe 2;

d) lorsque le sous-traitant n'est ni une institution ni un organe de l'Union, des règles d'entreprise contraignantes, des codes de conduite ou des mécanismes de certification, en vertu de l'article 46, paragraphe 2, points b), e) et f), du règlement (UE) 2016/679.

3. Sous réserve de l'autorisation du Contrôleur européen de la protection des données, les garanties appropriées visées au paragraphe 1 peuvent aussi être fournies, notamment, 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 à caractère personnel dans le pays tiers ou l'organisation internationale; ou

b) des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

4. Les autorisations accordées par le Contrôleur européen de la protection des données sur le fondement de l'article 9, paragraphe 7, du règlement (CE) n° 45/2001 demeurent valables jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par le Contrôleur européen de la protection des données.

5. Les institutions et organes de l'Union informent le Contrôleur européen de la protection des données des catégories de cas dans lesquels le présent article a été appliqué.

Article 49

Transferts ou divulgations non autorisés par le droit de l'Union

Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union, sans préjudice d'autres motifs de transfert en vertu du présent chapitre.

Article 50

Dérogations pour des situations particulières

1. En l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 ou de l'article 36, paragraphe 3, de la directive (UE) 2016/680, ou de garanties appropriées en vertu de l'article 48 du présent règlement, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes:

a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées;

b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée;

c) le transfert est 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 est nécessaire pour des motifs importants d'intérêt public;

e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice;

f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; ou

g) le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union, est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union sont remplies dans le cas d'espèce.

2. Les points a), b) et c) du paragraphe 1 ne s'appliquent pas aux activités menées par les institutions et organes de l'Union dans l'exercice de leurs prérogatives de puissance publique.

3. L'intérêt public visé au paragraphe 1, point d), est reconnu par le droit de l'Union.

4. 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, à moins que le droit de l'Union ne l'autorise. Lorsque le registre est destiné à être consulté par des personnes justifiant d'un intérêt légitime, le transfert n'est effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires.

5. En l'absence de décision d'adéquation, le droit de l'Union peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories spécifiques de données à caractère personnel vers un pays tiers ou à une organisation internationale.

6. Les institutions et organes de l'Union informent le Contrôleur européen de la protection des données des catégories de cas dans lesquels le présent article a été appliqué.

Article 51

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

En ce qui concerne les pays tiers et les organisations internationales, le Contrôleur européen de la protection des données, en concertation avec la Commission et le comité européen de la protection des données, prend les mesures appropriées pour:

a) élaborer des mécanismes de coopération internationale 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 l'application de la législation relative à la protection des données à caractère personnel, y compris par la notification, la transmission des réclamations, l'entraide pour les enquêtes et l'échange d'informations, 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 développer la coopération internationale dans le domaine de l'application de la législation relative à la protection des données à caractère personnel;

d) favoriser l'échange et la documentation de la législation et des pratiques en matière de protection des données à caractère personnel, y compris en ce qui concerne les conflits de compétence avec des pays tiers.

CHAPITRE VI

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Article 52

Contrôleur européen de la protection des données

1. La fonction de Contrôleur européen de la protection des données est instituée.

2. En ce qui concerne le traitement de données à caractère personnel, le Contrôleur européen de la protection des données est chargé de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union.

3. Le Contrôleur européen de la protection des données est chargé de contrôler et d'assurer l'application des dispositions du présent règlement et de tout autre acte de l'Union concernant la protection des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel effectués par une institution ou un organe de l'Union, ainsi que de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel. À ces fins, le Contrôleur européen de la protection des données remplit les missions prévues à l'article 57 et exerce les pouvoirs qui lui sont conférés à l'article 58.

4. Le règlement (CE) n° 1049/2001 s'applique aux documents détenus par le Contrôleur européen de la protection des données. Le Contrôleur européen de la protection des données adopte des modalités d'application du règlement (CE) n° 1049/2001 en ce qui concerne ces documents.

Article 53

Nomination du Contrôleur européen de la protection des données

1. Le Parlement européen et le Conseil nomment, d'un commun accord, le Contrôleur européen de la protection des données pour une durée de cinq ans, sur la base d'une liste établie par la Commission à la suite d'un appel public à candidatures. Cet appel à candidatures permet à toutes les personnes intéressées dans l'ensemble de l'Union de soumettre leur candidature. La liste des candidats établie par la Commission est publique et comporte au moins trois candidats. La commission compétente du Parlement européen, sur la base de la liste établie par la Commission, peut décider d'organiser une audition de manière à être en mesure d'émettre une préférence.

2. La liste de candidats visée au paragraphe 1 est constituée de personnes offrant toutes garanties d'indépendance et qui possèdent, de manière notoire, des connaissances spécialisées en matière de protection des données ainsi que l'expérience et les compétences requises pour l'exercice des fonctions de Contrôleur européen de la protection des données.

3. Le mandat du Contrôleur européen de la protection des données est renouvelable une fois.

4. Les fonctions du Contrôleur européen de la protection des données prennent fin dans les circonstances suivantes:

a) si le Contrôleur européen de la protection des données est remplacé;

b) si le Contrôleur européen de la protection des données démissionne;

c) si le Contrôleur européen de la protection des données est déclaré démissionnaire ou mis à la retraite d'office.

5. Le Contrôleur européen de la protection des données peut être déclaré démissionnaire ou déchu du droit à pension ou d'autres avantages en tenant lieu par la Cour, à la requête du Parlement européen, du Conseil ou de la Commission, s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions ou s'il a commis une faute grave.

6. Dans les cas de renouvellement régulier et de démission volontaire, le Contrôleur européen de la protection des données reste néanmoins en fonction jusqu'à ce qu'il soit pourvu à son remplacement.

7. Les articles 11 à 14 et 17 du protocole sur les privilèges et immunités de l'Union européenne s'appliquent au Contrôleur européen de la protection des données.

Article 54

Statut et conditions générales d'exercice des missions de Contrôleur européen de la protection des données, ressources humaines et financières

1. La fonction de Contrôleur européen de la protection des données est considérée comme équivalente à celle de juge de la Cour en ce qui concerne la détermination du traitement, des indemnités, de la pension d'ancienneté, et de tout autre avantage tenant lieu de rémunération.

2. L'autorité budgétaire veille à ce que le Contrôleur européen de la protection des données dispose des ressources humaines et financières nécessaires à l'exercice de ses missions.

3. Le budget du Contrôleur européen de la protection des données figure sur une ligne spécifique de la section relative aux dépenses administratives du budget général de l'Union.

4. Le Contrôleur européen de la protection des données est assisté par un secrétariat. Les fonctionnaires et les autres agents du secrétariat sont nommés par le Contrôleur européen de la protection des données, qui est leur supérieur hiérarchique. Ils en relèvent exclusivement. Leur nombre est arrêté chaque année dans le cadre de la procédure budgétaire. L'article 75, paragraphe 2, du règlement (UE) 2016/679 s'applique au personnel du Contrôleur européen de la protection des données chargé de mener à bien les missions conférées au comité européen de la protection des données par le droit de l'Union.

5. Les fonctionnaires et les autres agents du secrétariat du Contrôleur européen de la protection des données sont soumis aux règles et réglementations applicables aux fonctionnaires et autres agents de l'Union.

6. Le Contrôleur européen de la protection des données a son siège à Bruxelles.

Article 55

Indépendance

1. Le Contrôleur européen de la protection des données exerce en toute indépendance ses missions et ses pouvoirs conformément au présent règlement.

2. Dans l'exercice de ses missions et de ses pouvoirs conformément au présent règlement, le Contrôleur européen de la protection des données demeure libre de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicite ni n'accepte d'instructions de quiconque.

3. Le Contrôleur européen de la protection des données s'abstient de tout acte incompatible avec ses fonctions et, pendant la durée de celles-ci, ne peut exercer aucune autre activité professionnelle, rémunérée ou non.

4. Après la cessation de ses fonctions, le Contrôleur européen de la protection des données est tenu de respecter les devoirs d'honnêteté et de délicatesse quant à l'acceptation de certaines fonctions ou de certains avantages.

Article 56

Secret professionnel

Le Contrôleur européen de la protection des données et son personnel sont, pendant la durée de leurs fonctions et après la cessation de celles-ci, tenus au secret professionnel en ce qui concerne toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs fonctions officielles.

Article 57

Missions

1. Sans préjudice des autres missions prévues par le présent règlement, le Contrôleur européen de la protection des données:

a) contrôle et assure l'application du présent règlement par une institution ou un organe de l'Union, à l'exclusion du traitement de données à caractère personnel par la Cour dans l'exercice de ses fonctions juridictionnelles;

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

c) 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;

d) fournit, sur demande, à toute personne concernée des informations sur l'exercice des droits que lui confère le présent règlement et, si nécessaire, coopère, à cette fin, avec les autorités de contrôle nationales;

e) traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association, conformément à l'article 67, examine l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation 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;

f) 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;

g) conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel;

h) suit les évolutions pertinentes, 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 des communications;

i) adopte les clauses contractuelles types visées à l'article 29, paragraphe 8, et à l'article 48, paragraphe 2, point c);

j) établit et tient à jour une liste en lien avec l'obligation d'effectuer une analyse d'impact relative à la protection des données en application de l'article 39, paragraphe 4;

k) participe aux activités du comité européen de la protection des données;

l) assure le secrétariat du comité européen de la protection des données, conformément à l'article 75 du règlement (UE) 2016/679;

m) fournit des conseils concernant le traitement visé à l'article 40, paragraphe 2;

n) autorise les clauses contractuelles et les dispositions visées à l'article 48, paragraphe 3;

o) tient des registres internes des violations du présent règlement et des mesures prises conformément à l'article 58, paragraphe 2;

p) s'acquitte de toute autre mission relative à la protection des données à caractère personnel; et

q) établit son règlement intérieur.

2. Le Contrôleur européen de la protection des données facilite l'introduction des réclamations visées au paragraphe 1, point e), par la mise à disposition d'un formulaire de réclamation qui peut aussi être rempli par voie électronique, sans que d'autres moyens de communication ne soient exclus.

3. L'accomplissement des missions du Contrôleur européen de la protection des données est gratuit pour la personne concernée.

4. Lorsque les demandes sont manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif, le Contrôleur européen de la protection des données peut refuser d'y donner suite. Il incombe au Contrôleur européen de la protection des données de démontrer le caractère manifestement infondé ou excessif de la demande.

Article 58

Pouvoirs

1. Le Contrôleur européen de la protection des données dispose des pouvoirs d'enquête suivants:

a) ordonner au responsable du traitement et au sous-traitant de lui communiquer toute information dont il a besoin pour l'accomplissement de ses missions;

b) mener des enquêtes sous la forme d'audits sur la protection des données;

c) notifier au responsable du traitement ou au sous-traitant une violation alléguée du présent règlement;

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

e) obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation de traitement et à tout moyen de traitement, conformément au droit de l'Union.

2. Le Contrôleur européen de la protection des données dispose du pouvoir d'adopter les mesures correctrices suivantes:

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

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

c) saisir le responsable du traitement ou le sous-traitant concerné et, si nécessaire, le Parlement européen, le Conseil et la Commission;

d) ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement;

e) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé;

f) ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel;

g) imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;

h) ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en vertu des articles 18, 19 et 20 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 19, paragraphe 2, et de l'article 21;

i) imposer une amende administrative, en application de l'article 66, dans le cas où une institution ou un organe de l'Union ne se conformerait pas à l'une des mesures visées aux points d) à h) et j) du présent paragraphe, en fonction des circonstances propres à chaque cas;

j) ordonner la suspension des flux de données adressés à un destinataire situé dans un État membre ou un pays tiers ou à une organisation internationale.

3. Le Contrôleur européen de la protection des données dispose des pouvoirs d'autorisation et des pouvoirs consultatifs suivants:

a) conseiller les personnes concernées sur l'exercice de leurs droits;

b) conseiller le responsable du traitement conformément à la procédure de consultation préalable visée à l'article 40, et conformément à l'article 41, paragraphe 2;

c) émettre, de sa propre initiative ou sur demande, des avis à l'attention des institutions et organes de l'Union ainsi que du public, sur toute question relative à la protection des données à caractère personnel;

d) adopter les clauses types de protection des données visées à l'article 29, paragraphe 8, et à l'article 48, paragraphe 2, point c);

e) autoriser les clauses contractuelles visées à l'article 48, paragraphe 3, point a);

f) autoriser les arrangements administratifs visés à l'article 48, paragraphe 3, point b);

g) autoriser des opérations de traitement en vertu d'actes d'exécution adoptés au titre de l'article 40, paragraphe 4.

4. Le Contrôleur européen de la protection des données a le pouvoir de saisir la Cour dans les conditions prévues par les traités et d'intervenir dans les affaires portées devant la Cour.

5. L'exercice des pouvoirs conférés au Contrôleur européen de la protection des données en vertu du présent article est subordonné à des garanties appropriées, y compris le droit à un recours juridictionnel effectif et à une procédure régulière, prévu par le droit de l'Union.

Article 59

Obligation des responsables du traitement et des sous-traitants de répondre aux allégations

Lorsque le Contrôleur européen de la protection des données exerce les pouvoirs prévus à l'article 58, paragraphe 2, points a), b) et c), le responsable du traitement ou le sous-traitant concerné l'informe de son point de vue, dans un délai raisonnable que le Contrôleur européen de la protection des données aura fixé, en tenant compte des circonstances propres à chaque cas. Dans cet avis figure également une description des mesures prises, le cas échéant, en réponse aux observations du Contrôleur européen de la protection des données.

Article 60

Rapport d'activité

1. Le Contrôleur européen de la protection des données présente au Parlement européen, au Conseil et à la Commission un rapport annuel sur ses activités, qu'il rend public parallèlement.

2. Le Contrôleur européen de la protection des données transmet le rapport visé au paragraphe 1 aux autres institutions et organes de l'Union, qui peuvent présenter des observations en vue d'un éventuel examen du rapport par le Parlement européen.

CHAPITRE VII

COOPÉRATION ET COHÉRENCE

Article 61

Coopération entre le Contrôleur européen de la protection des données et les autorités de contrôle nationales

Le Contrôleur européen de la protection des données coopère avec les autorités de contrôle nationales ainsi qu'avec l'autorité de contrôle commune instituée en vertu de l'article 25 de la décision 2009/917/JAI du Conseil ([1]), dans la mesure nécessaire à l'exercice de leurs fonctions respectives, notamment en échangeant toute information utile, en se demandant mutuellement d'exercer leurs pouvoirs et en répondant aux demandes mutuelles de chacun.

Article 62

Contrôle coordonné exercé par le Contrôleur européen de la protection des données et les autorités de contrôle nationales

1. Lorsqu'un acte de l'Union renvoie au présent article, le Contrôleur européen de la protection des données et les autorités de contrôle nationales, agissant chacun dans les limites de leurs compétences respectives, coopèrent activement dans le cadre de leurs responsabilités afin d'assurer un contrôle effectif des systèmes d'information à grande échelle et des organes et organismes de l'Union.

2. Si nécessaire, agissant chacun dans les limites de leurs compétences respectives et dans le cadre de leurs responsabilités, ils échangent des informations utiles, se prêtent mutuellement assistance dans la réalisation d'audits et d'inspections, examinent les difficultés d'interprétation ou d'application du présent règlement et d'autres actes de l'Union applicables, étudient les problèmes liés à l'exercice d'un contrôle indépendant ou à l'exercice des droits des personnes concernées, définissent des propositions harmonisées visant à trouver des solutions aux problèmes éventuels et sensibilisent le public à la protection des données.

3. Aux fins prévues au paragraphe 2, le Contrôleur européen de la protection des données et les autorités de contrôle nationales se réunissent au moins deux fois par an dans le cadre du comité européen de la protection des données. À cet effet, le comité européen de la protection des données peut mettre au point d'autres méthodes de travail, si nécessaire.

4. Le comité européen de la protection des données transmet tous les deux ans un rapport conjoint relatif aux activités de contrôle coordonné au Parlement européen, au Conseil et à la Commission.

([1]) Décision 2009/917/JAI du Conseil du 30 novembre 2009 sur l'emploi de l'informatique dans le domaine des douanes (JO L 323 du 10.12.2009, p. 20).

CHAPITRE VIII

VOIES DE RECOURS, RESPONSABILITÉ ET SANCTIONS

Article 63

Droit d'introduire une réclamation auprès du Contrôleur européen de la protection des données

1. Sans préjudice de tout recours juridictionnel, administratif ou non juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès du Contrôleur européen de la protection des données si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement.

2. Le Contrôleur européen de la protection des données informe l'auteur 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 64.

3. Si le Contrôleur européen de la protection des données ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation, il est réputé avoir adopté une décision négative.

Article 64

Droit à un recours juridictionnel effectif

1. La Cour est compétente pour connaître de tout litige relatif aux dispositions du présent règlement, y compris les demandes d'indemnisation.

2. Les décisions du Contrôleur européen de la protection des données, y compris les décisions rendues au titre de l'article 63, paragraphe 3, peuvent faire l'objet d'un recours devant la Cour.

3. La Cour dispose d'une compétence de pleine juridiction pour statuer sur les recours formés contre les amendes administratives visées à l'article 66. Elle peut annuler, réduire ou majorer ces amendes dans les limites fixées à l'article 66.

Article 65

Droit à réparation

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir de l'institution ou l'organe de l'Union la réparation du dommage subi, sous réserve des conditions prévues dans les traités.

Article 66

Amendes administratives

1. Le Contrôleur européen de la protection des données peut imposer des amendes administratives aux institutions et organes de l'Union, en fonction des circonstances propres à chaque cas, lorsqu'une institution ou un organe de l'Union ne respecte pas une injonction du Contrôleur européen de la protection des données émise en vertu de l'article 58, paragraphe 2, points d) à h) et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, 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 du nombre de personnes concernées affectées et du niveau de dommage qu'elles ont subi;

b) toute mesure prise par l'institution ou l'organe de l'Union pour atténuer le dommage subi par les personnes concernées;

c) le degré de responsabilité de l'institution ou de l'organe de l'Union, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en application des articles 27 et 33;

d) toute violation similaire commise précédemment par l'institution ou l'organe de l'Union;

e) le degré de coopération établi avec le Contrôleur européen de la protection des données en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;

f) les catégories de données à caractère personnel concernées par la violation;

g) la manière dont le Contrôleur européen de la protection des données a eu connaissance de la violation, notamment si, et dans quelle mesure, l'institution ou l'organe de l'Union a notifié la violation;

h) le respect de l'une ou l'autre des mesures visées à l'article 58 qui ont été précédemment ordonnées à l'encontre de l'institution ou de l'organe de l'Union concerné pour le même objet. Les procédures conduisant à imposer ces amendes sont menées dans un délai raisonnable en fonction des circonstances propres à chaque cas, en tenant compte des actions et procédures applicables visées à l'article 69.

2. Toute violation des obligations de l'institution ou de l'organe de l'Union prévues aux articles 8, 12, 27 à 35, 39, 40, 43, 44 et 45 fait l'objet, conformément au paragraphe 1 du présent article, d'amendes administratives pouvant s'élever jusqu'à 25 000 EUR par violation et 250 000 EUR par an au total.

3. Toute violation des dispositions suivantes par l'institution ou l'organe de l'Union fait l'objet, conformément au paragraphe 1, d'amendes administratives pouvant s'élever jusqu'à 50 000 EUR par violation et 500 000 EUR par an au total:

a) les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 4, 5, 7 et 10;

b) les droits dont bénéficient les personnes concernées en vertu des articles 14 à 24:

c) les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale visés aux articles 46 à 50.

4. Si une institution ou un organe de l'Union viole plusieurs dispositions du présent règlement ou plusieurs fois la même disposition du présent règlement, dans le cadre de la même opération de traitement ou d'opérations de traitement liées ou continues, le montant total de l'amende administrative ne peut excéder le montant fixé pour la violation la plus grave.

5. Avant de prendre des décisions en vertu du présent article, le Contrôleur européen de la protection des données donne à l'institution ou à l'organe de l'Union faisant l'objet des procédures conduites par le Contrôleur européen de la protection des données la possibilité de faire connaître son point de vue au sujet des griefs que le Contrôleur européen de la protection des données a retenus. Le Contrôleur européen de la protection des données ne fonde ses décisions que sur les griefs au sujet desquels les parties concernées ont pu formuler des observations. Les plaignants sont étroitement associés à la procédure.

6. Les droits de la défense des parties concernées sont pleinement respectés dans le déroulement de la procédure. Les parties disposent d'un droit d'accès au dossier du Contrôleur européen de la protection des données, sous réserve de l'intérêt légitime des personnes ou entreprises concernées en ce qui concerne la protection de leurs données à caractère personnel ou de leurs secrets commerciaux.

7. Les fonds collectés en imposant des amendes en vertu du présent article font partie des recettes du budget général de l'Union.

Article 67

Représentation des personnes concernées

La personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit de l'Union ou au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées en ce qui concerne la protection des données à caractère personnel les concernant, pour qu'il introduise une réclamation en son nom auprès du Contrôleur européen de la protection des données, exerce en son nom les droits prévus aux articles 63 et 64 et exerce en son nom le droit d'obtenir réparation prévu à l'article 65.

Article 68

Réclamations du personnel de l'Union

Toute personne employée par une institution ou un organe de l'Union peut présenter une réclamation au Contrôleur européen de la protection des données pour une violation alléguée des dispositions du présent règlement, y compris sans passer par les voies officielles. Nul ne doit subir de préjudice pour avoir présenté au Contrôleur européen de la protection des données une réclamation alléguant une telle violation.

Article 69

Sanctions

Lorsqu'un fonctionnaire ou un autre agent de l'Union manque aux obligations prévues dans le présent règlement intentionnellement ou par négligence, le fonctionnaire ou autre agent concerné est passible d'une sanction disciplinaire ou d'une autre sanction, conformément aux dispositions du statut.

CHAPITRE IX

TRAITEMENT DES DONNÉES OPÉRATIONNELLES À CARACTÈRE PERSONNEL PAR LES ORGANES ET ORGANISMES DE L'UNION DANS L'EXERCICE D'ACTIVITÉS QUI RELÈVENT DU CHAMP D'APPLICATION DE LA TROISIÈME PARTIE, TITRE V, CHAPITRE 4 OU 5, DU TRAITÉ SUR LE FONCTIONNEMENT DE L'UNION EUROPÉENNE

Article 70

Champ d'application du chapitre

Le présent chapitre s'applique uniquement au traitement des données opérationnelles à caractère personnel par les organes et organismes de l'Union dans l'exercice d'activités qui relèvent du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne, sans préjudice des règles spécifiques en matière de protection des données applicables à ces organes ou organismes de l'Union.

Article 71

Principes relatifs au traitement des données opérationnelles à caractère personnel

1. Les données opérationnelles à caractère personnel doivent être:

a) traitées de manière licite et loyale (licéité et loyauté);

b) collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités (limitation des finalités);

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

d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données opérationnelles à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles les données opérationnelles à caractère personnel sont traitées (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données opérationnelles à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le traitement, par le même ou par un autre responsable du traitement, pour l'une ou l'autre des finalités énoncées dans l'acte juridique instituant l'organe ou l'organisme de l'Union, autre que celles pour lesquelles les données opérationnelles à caractère personnel ont été collectées, est autorisé à condition que:

a) le responsable du traitement soit autorisé à traiter ces données opérationnelles à caractère personnel pour une telle finalité conformément au droit de l'Union; et

b) le traitement soit nécessaire et proportionné à cette autre finalité conformément au droit de l'Union.

3. Le traitement par le même ou par un autre responsable du traitement peut comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, aux fins énoncées dans l'acte juridique instituant l'organe ou l'organisme de l'Union, sous réserve de garanties appropriées pour les droits et libertés des personnes concernées.

4. Le responsable du traitement est responsable du respect des paragraphes 1, 2 et 3 et est en mesure de démontrer que ces dispositions sont respectées.

Article 72

Licéité du traitement des données opérationnelles à caractère personnel

1. Le traitement des données opérationnelles à caractère personnel n'est licite que si, et dans la mesure où, il est nécessaire à l'exécution d'une mission effectuée par des organes et organismes de l'Union dans l'exercice d'activités qui relèvent du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne, et il est fondé sur le droit de l'Union.

2. Les actes juridiques spécifiques de l'Union qui régissent le traitement dans le cadre du champ d'application du présent chapitre précisent au moins les objectifs du traitement, les données opérationnelles à caractère personnel à traiter, les finalités du traitement et les délais de conservation des données opérationnelles à caractère personnel ou les délais de vérification régulière de la nécessité de conserver les données opérationnelles à caractère personnel.

Article 73

Distinction entre différentes catégories de personnes concernées

Le responsable du traitement établit, le cas échéant et dans la mesure du possible, une distinction claire entre les données opérationnelles à caractère personnel de différentes catégories de personnes concernées, telles que les catégories prévues dans les actes juridiques instituant les organes et organismes de l'Union.

Article 74

Distinction entre les données opérationnelles à caractère personnel et vérification de la qualité des données opérationnelles à caractère personnel

1. Le responsable du traitement établit, dans la mesure du possible, une distinction entre les données opérationnelles à caractère personnel fondées sur des faits et celles fondées sur des appréciations personnelles.

2. Le responsable du traitement prend toutes les mesures raisonnables pour garantir que les données opérationnelles à caractère personnel qui sont inexactes, incomplètes ou qui ne sont plus à jour ne soient pas transmises ou mises à disposition. À cette fin, le responsable du traitement vérifie, dans la mesure du possible et s'il y a lieu, la qualité des données opérationnelles à caractère personnel avant leur transmission ou mise à disposition, par exemple, en consultant l'autorité compétente d'où proviennent les données. Dans la mesure du possible, lors de toute transmission de données opérationnelles à caractère personnel, le responsable du traitement ajoute les informations nécessaires pour permettre au destinataire de juger du degré d'exactitude, d'exhaustivité et de fiabilité des données opérationnelles à caractère personnel, et de leur niveau de mise à jour.

3. S'il s'avère que des données opérationnelles à caractère personnel inexactes ont été transmises ou que des données opérationnelles à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données opérationnelles à caractère personnel concernées sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 82.

Article 75

Conditions spécifiques applicables au traitement

1. Lorsque le droit de l'Union applicable au responsable du traitement qui transmet les données soumet le traitement à des conditions spécifiques, le responsable du traitement informe le destinataire de ces données opérationnelles à caractère personnel de ces conditions et de l'obligation de les respecter.

2. Le responsable du traitement respecte les conditions spécifiques applicables au traitement prévues par une autorité compétente qui transmet les données, conformément à l'article 9, paragraphes 3 et 4, de la directive (UE) 2016/680.

Article 76

Traitement portant sur des catégories particulières de données opérationnelles à caractère personnel

1. Le traitement des données opérationnelles à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données opérationnelles à caractère personnel concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique est autorisé uniquement en cas de nécessité absolue à des fins opérationnelles dans le cadre du mandat de l'organe ou de l'organisme de l'Union concerné et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée. La discrimination à l'égard de personnes physiques sur la base de ces données à caractère personnel est interdite.

2. Le délégué à la protection des données est informé dans les meilleurs délais du recours au présent article.

Article 77

Décision individuelle automatisée, y compris le profilage

1. Toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative est interdite, à moins qu'elle ne soit autorisée par une disposition du droit de l'Union à laquelle le responsable du traitement est soumis et qui fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement.

2. Les décisions visées au paragraphe 1 du présent article ne sont pas fondées sur les catégories particulières de données à caractère personnel visées à l'article 76, à moins que des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée ne soient en place.

3. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 76 est interdit, conformément au droit de l'Union.

Article 78

Communication et modalités de l'exercice des droits de la personne concernée

1. Le responsable du traitement prend des mesures raisonnables pour fournir toute information visée à l'article 79 et procède à toute communication au titre des articles 80 à 84 et de l'article 92 en ce qui concerne le traitement à la personne concernée d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par tout moyen approprié, y compris par voie électronique. De manière générale, le responsable du traitement fournit les informations sous la même forme que la demande.

2. Le responsable du traitement facilite l'exercice des droits de la personne concernée au titre des articles 79 à 84.

3. Le responsable du traitement informe par écrit la personne concernée de la suite réservée à sa demande, dans les meilleurs délais, et en tout état de cause au plus tard trois mois après réception de la demande de la personne concernée.

4. Le responsable du traitement fournit les informations visées à l'article 79 et procède à toute communication et prend toute mesure au titre des articles 80 à 84 et de l'article 92 à titre gratuit. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut refuser de donner suite à la demande. Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

5. Lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée à l'article 80 ou 82, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

Article 79

Informations à mettre à la disposition de la personne concernée ou à lui fournir

1. Le responsable du traitement met à la disposition de la personne concernée au moins les informations suivantes:

a) l'identité et les coordonnées de l'organe ou de l'organisme de l'Union;

b) les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données opérationnelles à caractère personnel;

d) le droit d'introduire une réclamation auprès du Contrôleur européen de la protection des données et les coordonnées de ce dernier;

e) l'existence du droit de demander au responsable du traitement l'accès aux données opérationnelles à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données opérationnelles à caractère personnel relatives à la personne concernée.

2. Outre les informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée, dans des cas particuliers prévus par le droit de l'Union, les informations supplémentaires suivantes afin de lui permettre d'exercer ses droits:

a) la base juridique du traitement,

b) la durée de conservation des données opérationnelles à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

c) le cas échéant, les catégories de destinataires des données opérationnelles à caractère personnel, y compris dans les pays tiers ou au sein d'organisations internationales;

d) au besoin, d'autres informations, en particulier lorsque les données opérationnelles à caractère personnel sont collectées à l'insu de la personne concernée.

3. Le responsable du traitement peut retarder ou limiter la fourniture des informations à la personne concernée en application du paragraphe 2, ou ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour:

a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;

b) éviter de nuire à la prévention et à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière, ou à l'exécution de sanctions pénales;

c) protéger la sécurité publique des États membres;

d) protéger la sécurité nationale des États membres;

e) protéger les droits et libertés d'autrui, tel que les victimes et les témoins.

Article 80

Droit d'accès de la personne concernée

La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données opérationnelles à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, elle a le droit d'avoir accès auxdites données opérationnelles à caractère personnel et d'obtenir les informations suivantes:

a) les finalités du traitement ainsi que sa base juridique;

b) les catégories de données opérationnelles à caractère personnel concernées;

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

d) lorsque cela est possible, la durée de conservation des données opérationnelles à caractère personnel envisagée ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée;

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

f) le droit de d'introduire une réclamation auprès du Contrôleur européen de la protection des données et les coordonnées de ce dernier;

g) la communication des données opérationnelles à caractère personnel en cours de traitement, ainsi que toute information disponible sur l'origine de ces données.

Article 81

Limitations du droit d'accès

1. Le responsable du traitement peut limiter, entièrement ou partiellement, le droit d'accès de la personne concernée, dès lors et aussi longtemps qu'une telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour:

a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;

b) éviter de nuire à la prévention et à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière, ou à l'exécution de sanctions pénales;

c) protéger la sécurité publique des États membres;

d) protéger la sécurité nationale des États membres;

e) protéger les droits et libertés d'autrui, tel que les victimes et témoins.

2. Dans les cas visés au paragraphe 1, le responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, de tout refus ou de toute limitation d'accès, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au paragraphe 1. Le responsable du traitement informe la personne concernée de la possibilité d'introduire une réclamation auprès du Contrôleur européen de la protection des données ou de former un recours juridictionnel devant la Cour. Le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition du Contrôleur européen de la protection des données sur demande.

Article 82

Droit de rectification ou d'effacement des données opérationnelles à caractère personnel et limitation du traitement

1. Toute personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données opérationnelles à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données opérationnelles à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

2. Le responsable du traitement efface, dans les meilleurs délais, les données opérationnelles à caractère personnel et la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant lorsque le traitement constitue une violation de l'article 71, de l'article 72, paragraphe 1, ou de l'article 76, ou lorsque les données opérationnelles à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.

3. Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement lorsque:

a) l'exactitude des données à caractère personnel est contestée par la personne concernée et il ne peut être déterminé si les données sont exactes ou non; ou

b) les données à caractère personnel doivent être conservées à des fins probatoires.

Lorsque le traitement est limité en vertu du premier alinéa, point a), le responsable du traitement informe la personne concernée avant de lever la limitation du traitement.

Les données soumises à limitation ne sont traitées que pour les finalités qui ont empêché leur effacement.

4. Le responsable du traitement informe la personne concernée par écrit de tout refus de rectifier ou d'effacer des données opérationnelles à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus. Le responsable du traitement peut limiter, entièrement ou partiellement, la fourniture de ces informations dès lors qu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour:

a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;

b) éviter de nuire à la prévention et à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière, ou à l'exécution de sanctions pénales;

c) protéger la sécurité publique des États membres;

d) protéger la sécurité nationale des États membres;

e) protéger les droits et libertés d'autrui, tel que les victimes et les témoins.

Le responsable du traitement informe la personne concernée de la possibilité d'introduire une réclamation auprès du Contrôleur européen de la protection des données ou de former un recours juridictionnel devant la Cour.

5. Le responsable du traitement communique la rectification des données opérationnelles à caractère personnel inexactes à l'autorité compétente d'où proviennent les données opérationnelles à caractère personnel inexactes.

6. Lorsque des données opérationnelles à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité en application des paragraphe 1, 2 ou 3, le responsable du traitement adresse une notification aux destinataires et les informe qu'ils doivent rectifier ou effacer les données opérationnelles à caractère personnel ou limiter le traitement des données opérationnelles à caractère personnel sous leur responsabilité.

Article 83

Droit d'accès dans le cadre des enquêtes et des procédures pénales

Lorsque les données opérationnelles à caractère personnel proviennent d'une autorité compétente, les organes et organismes de l'Union, avant de prendre une décision sur le droit d'accès d'une personne concernée, vérifient avec l'autorité compétente concernée si ces données à caractère personnel figurent dans une décision judiciaire ou un casier ou dossier judiciaire faisant l'objet d'un traitement lors d'une enquête et d'une procédure pénale dans l'État membre de cette autorité compétente. Si tel est le cas, une décision sur le droit d'accès est prise en consultation et en étroite coopération avec l'autorité compétente concernée.

Article 84

Exercice des droits de la personne concernée et vérification par le Contrôleur européen de la protection des données

1. Dans les cas visés à l'article 79, paragraphe 3, à l'article 81 et à l'article 82, paragraphe 4, les droits de la personne concernée peuvent également être exercés par l'intermédiaire du Contrôleur européen de la protection des données.

2. Le responsable du traitement informe la personne concernée de la possibilité qu'elle a d'exercer ses droits par l'intermédiaire du Contrôleur européen de la protection des données en application du paragraphe 1.

3. Lorsque le droit visé au paragraphe 1 est exercé, le Contrôleur européen de la protection des données informe au moins la personne concernée du fait qu'il a procédé à toutes les vérifications nécessaires ou à un examen. Le Contrôleur européen de la protection des données informe également la personne concernée de son droit de former un recours juridictionnel devant la Cour.

Article 85

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

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et les libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de l'acte juridique qui l'a institué et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données opérationnelles à caractère personnel qui sont adéquates, pertinentes et non excessives au regard de la finalité du traitement sont traitées. Cette obligation s'applique à la quantité de données opérationnelles à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données opérationnelles à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

Article 86

Responsables conjoints du traitement

1. Lorsque deux ou plusieurs responsables du traitement ou un ou plusieurs responsables du traitement avec un ou plusieurs responsables du traitement autres que les institutions et organes de l'Union, déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs responsabilités respectives quant au respect des obligations qui leur incombent en matière de protection des données, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées à l'article 79, par voie d'accord entre eux, sauf si, et dans la mesure où, leurs responsabilités respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables conjoints du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

2. L'accord mentionné au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis de la personne concernée. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

3. 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 de et contre chacun des responsables du traitement.

Article 87

Sous-traitant

1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées pour que le traitement réponde aux exigences du présent règlement et de l'acte juridique instituant le responsable du traitement et garantisse la protection des droits de la personne concernée.

2. Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe 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.

3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement et qui définit l'objet, la durée, la nature et la finalité du traitement, le type de données opérationnelles à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant:

a) n'agit que sur instruction du responsable du traitement;

b) veille à ce que les personnes autorisées à traiter les données opérationnelles à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;

c) aide le responsable du traitement, par tout moyen approprié, à veiller au respect des dispositions relatives aux droits de la personne concernée;

d) selon le choix du responsable du traitement, supprime toutes les données opérationnelles à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit d'un État membre n'exige la conservation des données opérationnelles à caractère personnel;

e) 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;

f) respecte les conditions visées au paragraphe 2 et au présent paragraphe pour recruter un autre sous-traitant.

4. Le contrat ou l'autre acte juridique visé au paragraphe 3 se présente sous forme écrite, y compris sous forme électronique.

5. Si, en violation du présent règlement ou de l'acte juridique instituant le responsable du traitement, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement.

Article 88

Journalisation

1. Le responsable du traitement établit des journaux pour les opérations de traitement ci-après effectuées dans des systèmes de traitement automatisé: la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement des données opérationnelles à caractère personnel et l'accès à celles-ci. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de ces opérations, l'identification de la personne qui a consulté ou communiqué les données opérationnelles à caractère personnel, ainsi que, dans la mesure du possible, l'identité des destinataires de ces données opérationnelles à caractère personnel.

2. Les journaux sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données opérationnelles à caractère personnel et à des fins de procédures pénales. Ces journaux sont effacés au bout de trois ans, sauf s'ils demeurent nécessaires à un contrôle en cours.

3. Le responsable du traitement met les journaux à la disposition de son délégué à la protection des données et du Contrôleur européen de la protection des données sur demande.

Article 89

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'engendrer un risque élevé pour les droits et les libertés des personnes physiques, le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données opérationnelles à caractère personnel.

2. L'analyse visée au paragraphe 1 contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et les libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données opérationnelles à caractère personnel et à apporter la preuve du respect des règles de protection des données, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées.

Article 90

Consultation préalable du Contrôleur européen de la protection des données

1. Le responsable du traitement consulte le Contrôleur européen de la protection des données préalablement au traitement qui fera partie d'un nouveau fichier à créer:

a) lorsqu'une analyse d'impact relative à la protection des données effectuée en vertu de l'article 89 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; ou

b) lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.

2. Le Contrôleur européen de la protection des données peut établir une liste des opérations de traitement devant faire l'objet d'une consultation préalable conformément au paragraphe 1.

3. Le responsable du traitement fournit au Contrôleur européen de la protection des données l'analyse d'impact relative à la protection des données visée à l'article 89 et, sur demande, toute autre information afin de permettre au Contrôleur européen de la protection des données d'apprécier la conformité du traitement et, en particulier, les risques pour la protection des données opérationnelles à caractère personnel de la personne concernée et les garanties qui s'y rapportent.

4. Lorsque le Contrôleur européen de la protection des données est d'avis que le traitement envisagé, visé au paragraphe 1, constituerait une violation du présent règlement ou de l'acte juridique instituant l'organe ou l'organisme de l'Union, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, le Contrôleur européen de la protection des données fournit un avis écrit au responsable du traitement, dans un délai maximum de six semaines à compter de la réception de la demande de consultation. Ce délai peut être prolongé d'un mois, en fonction de la complexité du traitement envisagé. Le Contrôleur européen de la protection des données informe le responsable du traitement de toute prorogation dans un délai d'un mois à compter de la réception de la demande de consultation ainsi que des motifs du retard.

Article 91

Sécurité du traitement des données opérationnelles à caractère personnel

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et les libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données opérationnelles à caractère personnel.

2. En ce qui concerne le traitement automatisé, le responsable du traitement et le sous-traitant mettent en œuvre, à la suite d'une évaluation des risques, des mesures destinées à:

a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données (contrôle de l'accès aux installations);

b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);

c) empêcher l'introduction non autorisée de données opérationnelles à caractère personnel ainsi que tout examen, toute modification ou tout effacement non autorisés de données opérationnelles à caractère personnel conservées (contrôle de la conservation);

d) empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs);

e) garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données opérationnelles à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données);

f) garantir qu'il puisse être vérifié et constaté à quelles instances des données opérationnelles à caractère personnel ont été ou peuvent être transmises ou mises à disposition par transmission de données (contrôle de la transmission);

g) garantir qu'il puisse être vérifié et constaté a posteriori quelles données opérationnelles à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction);

h) empêcher que, lors de la transmission de données opérationnelles à caractère personnel ainsi que lors du transport de supports de données, les données opérationnelles à caractère personnel puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);

i) garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration);

j) garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données opérationnelles à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).

Article 92

Notification au Contrôleur européen de la protection des données d'une violation de données à caractère personnel

1. En cas de violation de données à caractère personnel, le responsable du traitement notifie la violation en question au Contrôleur européen de la protection des données dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification au Contrôleur européen de la protection des données n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. 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, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données opérationnelles à caractère personnel concernés;

b) indiquer le nom et les coordonnées du délégué à la protection des données;

c) décrire les conséquences probables de la violation de données à caractère personnel;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, s'il y a lieu, les mesures pour en atténuer les éventuelles conséquences négatives.

3. Lorsque, et dans la mesure où, il n'est pas possible de fournir les informations visées au paragraphe 2 en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

4. Le responsable du traitement documente toute violation de données à caractère personnel visée au paragraphe 1, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet au Contrôleur européen de la protection des données de vérifier le respect du présent article.

5. Lorsque la violation de données à caractère personnel porte sur des données opérationnelles à caractère personnel qui ont été transmises par les autorités compétentes ou à celles-ci, le responsable du traitement communique les informations visées au paragraphe 2 aux autorités compétentes concernées dans les meilleurs délais.

Article 93

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

1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et les recommandations visées à l'article 92, paragraphe 2, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces dernières ont été appliquées aux données opérationnelles à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données opérationnelles à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

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

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, le Contrôleur européen de la protection des données peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une des conditions visées au paragraphe 3 est remplie.

5. La communication à la personne concernée visée au paragraphe 1 du présent article peut être retardée, limitée ou omise, sous réserve des conditions et pour les motifs visés à l'article 79, paragraphe 3.

Article 94

Transfert de données opérationnelles à caractère personnel à des pays tiers ou à des organisations internationales

1. Sous réserve des restrictions et conditions prévues dans les actes juridiques instituant l'organe ou l'organisme de l'Union, le responsable du traitement peut transférer des données opérationnelles à caractère personnel à une autorité d'un pays tiers ou à une organisation internationale, dans la mesure où ce transfert est nécessaire à l'exécution des tâches du responsable du traitement, et uniquement lorsque les conditions fixées au présent article sont remplies, à savoir:

a) la Commission a adopté, conformément à l'article 36, paragraphe 3, de la directive (UE) 2016/680, une décision d'adéquation selon laquelle le pays tiers ou un territoire ou un secteur de traitement de données au sein de ce pays tiers, ou l'organisation internationale en question, assure un niveau de protection adéquat;

b) en l'absence de décision d'adéquation de la Commission visée au point a), un accord international a été conclu entre l'Union et le pays tiers ou l'organisation internationale concerné, en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne, offrant des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes;

c) en l'absence de décision d'adéquation de la Commission en vertu du point a) ou d'accord international en vertu du point b), un accord de coopération autorisant l'échange de données opérationnelles à caractère personnel a été conclu avant la date d'application de l'acte juridique instituant l'organe ou l'organisme de l'Union concerné, entre cet organe ou organisme de l'Union et le pays tiers en question.

2. Les actes juridiques instituant les organes et organismes de l'Union peuvent maintenir ou introduire des dispositions plus précises sur les conditions relatives aux transferts internationaux de données opérationnelles à caractère personnel, en particulier sur les transferts faisant l'objet de garanties appropriées et de dérogations pour des situations particulières.

3. Le responsable du traitement publie sur son site internet et tient à jour une liste des décisions d'adéquation visées au paragraphe 1, point a), des accords, des arrangements administratifs et des autres instruments relatifs au transfert de données opérationnelles à caractère personnel conformément au paragraphe 1.

4. Le responsable du traitement tient un relevé détaillé de tous les transferts effectués au titre du présent article.

Article 95

Secret des enquêtes judiciaires et des procédures pénales

Les actes juridiques instituant les organes ou organismes de l'Union exerçant des activités qui relèvent du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne peuvent contraindre le Contrôleur européen de la protection des données, dans l'exercice de ses pouvoirs de contrôle, à tenir le plus grand compte du secret des enquêtes judiciaires et des procédures pénales, conformément au droit de l'Union ou au droit des États membres.

CHAPITRE X

ACTES D'EXÉCUTION

Article 96

Comité

1. La Commission est assistée par le comité institué par l'article 93 du règlement (UE) 2016/679. Ledit 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) n° 182/2011 s'applique.

CHAPITRE XI

RÉEXAMEN

Article 97

Clause de réexamen

Le 30 avril 2022 au plus tard, puis tous les cinq ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'application du présent règlement, accompagné, le cas échéant, des propositions législatives appropriées.

Article 98

Réexamen des actes juridiques de l'Union

1. Le 30 avril 2022 au plus tard, la Commission réexamine les actes juridiques adoptés sur la base des traités qui régissent le traitement de données opérationnelles à caractère personnel par les organes ou organismes de l'Union lorsqu'elles exercent des activités qui relèvent du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne, afin de:

a) s'assurer de leur compatibilité avec la directive (UE) 2016/680 et avec le chapitre IX du présent règlement;

b) recenser les divergences qui sont susceptibles d'entraver l'échange de données opérationnelles à caractère personnel entre les organes ou organismes de l'Union lorsqu'elles exercent des activités dans ces domaines et les autorités compétentes; et

c) identifier les divergences qui sont susceptibles de donner lieu à une fragmentation juridique de la législation en matière de protection des données dans l'Union.

2. Sur la base de ce réexamen, pour assurer une protection uniforme et cohérente des personnes physiques à l'égard du traitement, la Commission peut présenter des propositions législatives appropriées, notamment en vue d'appliquer le chapitre IX du présent règlement à Europol et au Parquet européen, y compris des adaptations du chapitre IX, si nécessaire.

CHAPITRE XII

DISPOSITIONS FINALES

Article 99

Abrogation du règlement (CE) n° 45/2001 et de la décision n° 1247/2002/CE.

Le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE sont abrogés avec effet au 11 décembre 2018. Les références faites au règlement et à la décision abrogés s'entendent comme faites au présent règlement.

Article 100

Mesures transitoires

1. Le présent règlement ne porte pas atteinte à la décision 2014/886/UE du Parlement européen et du Conseil ([1]) ni aux mandats actuels du Contrôleur européen de la protection des données et du Contrôleur adjoint.

([1]) Décision 2014/886/UE du Parlement européen et du Conseil du 4 décembre 2014 portant nomination du contrôleur européen de la protection des données et du contrôleur adjoint (JO L 351 du 9.12.2014, p. 9).

2. La fonction de Contrôleur adjoint est considérée comme équivalente à celle de greffier de la Cour en ce qui concerne la détermination du traitement, des indemnités, de la pension d'ancienneté, et de tout autre avantage tenant lieu de rémunération.

3. L'article 53, paragraphes 4, 5 et 7, et les articles 55 et 56 du présent règlement s'appliquent à l'actuel Contrôleur adjoint jusqu'à la fin de son mandat.

4. Le Contrôleur adjoint assiste le Contrôleur européen de la protection des données dans l'ensemble de ses fonctions et le supplée en cas d'absence ou d'empêchement jusqu'à la fin du mandat de l'actuel Contrôleur adjoint.

Article 101

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. Toutefois, le présent règlement s'applique au traitement de données à caractère personnel par Eurojust à partir du 12 décembre 2019.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le 23 octobre 2018.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
A. TAJANI	K. EDTSTADLER