Conseil de
l'Union européenne

Bruxelles, le 12 janvier 2017
(OR. en)

5034/17

Dossier interinstitutionnel:
2017/0002 (COD)

DATAPROTECT 2
JAI 2
DAPIX 2
FREMP 1
DIGIT 2
CODEC 4

PROPOSITION

Origine:	Pour le Secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, Directeur
Date de réception:	12 janvier 2017
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, Secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2017) 8 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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

Les délégations trouveront ci-joint le document COM(2017) 8 final.

p.j.: COM(2017) 8 final

COMMISSION
EUROPÉENNE

Bruxelles, le 10.1.2017
COM(2017) 8 final

2017/0002 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

L'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE), introduit par le traité de Lisbonne, établit le principe selon lequel toute personne a droit à la protection des données à caractère personnel la concernant. En outre, avec l'article 16, paragraphe 2, du TFUE, le traité de Lisbonne a créé une base juridique spécifique pour l'adoption de règles en matière de protection des données à caractère personnel. L'article 8 de la charte des droits fondamentaux de l'Union européenne consacre la protection des données à caractère personnel en tant que droit fondamental.

Le droit à la protection des données à caractère personnel s'applique également au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union. Le règlement (CE) n° 45/2001[1], principal instrument législatif de l'UE en matière de protection des données à caractère personnel dans les institutions de l'Union, avait été adopté en 2001 avec deux objectifs à l'esprit: protéger le droit fondamental à la protection des données et garantir la libre circulation des données à caractère personnel au sein de l'Union. Il a été complété par la décision n° 1247/2002/CE[2].

Le 27 avril 2016, le Parlement européen et le Conseil ont adopté le règlement général sur la protection des données [règlement (UE) 2016/679], qui sera applicable à partir du 25 mai 2018. Ce règlement demande une adaptation du règlement (CE) n° 45/2001 aux principes et aux règles fixés dans le règlement (UE) 2016/679 afin de mettre en place un cadre de protection des données solide et cohérent dans l'Union et de permettre aux deux instruments d'être appliqués en même temps[3].

Il s'inscrit dans le cadre de l'approche cohérente de la protection des données à caractère personnel dans l'ensemble de l'Union visant à aligner, autant que possible, les règles en matière de protection des données pour les institutions, organes et organismes de l'Union sur les règles relatives à la protection des données adoptées pour les États membres. Chaque fois que les dispositions de la proposition se fondent sur le même concept que les dispositions du règlement (UE) 2016/679, ces deux dispositions devraient être interprétées de manière homogène, notamment en raison du fait que l'économie de la proposition devrait être comprise comme le pendant de l'économie du règlement (UE) 2016/679[4].

Le réexamen du règlement (CE) n° 45/2001 tient également compte des résultats des enquêtes et des consultations des parties prenantes, et de l'étude d'évaluation sur son application au cours des 15 dernières années.

---

1 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.

2 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.

3 Voir règlement (UE) 2016/679, article 98 et considérant 17.

4 Voir l'arrêt de la Cour du 9 mars 2010, Commission/Allemagne, C-518/07, ECLI:EU:C:2010:125, points 26 et 28.

Cette initiative ne relève pas du programme pour une réglementation affûtée et performante (REFIT).

- **Cohérence par rapport aux dispositions existantes dans le domaine d'action**

La proposition vise à aligner les dispositions du règlement (CE) n° 45/2001 sur les principes et règles prévus par le règlement (UE) 2016/679 afin de mettre en place un cadre de protection des données solide et cohérent dans l'Union. La proposition intègre également les règles pertinentes établies dans le règlement (CE) XXXX/XX [règlement «vie privée et communications électroniques»] en ce qui concerne la protection des équipements terminaux des utilisateurs finals.

- **Cohérence par rapport aux autres politiques de l'Union**

Sans objet

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant est un droit fondamental consacré par l'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne.

La présente proposition est fondée sur l'article 16 du TFUE, qui est la base juridique pour l'adoption de règles en matière de protection des données. Cet article permet d'adopter des règles relatives 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 dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union. Il permet également l'adoption de règles relatives à la libre circulation de ces données, y compris les données à caractère personnel traitées par ces institutions, organes et organismes.

- **Subsidiarité (en cas de compétence non exclusive)**

L'objet du présent règlement relève de la compétence exclusive de l'Union, étant donné que seule l'Union peut adopter une réglementation régissant le traitement des données à caractère personnel par les institutions de l'Union.

- **Proportionnalité**

Conformément au principe de proportionnalité, en vue d'atteindre les objectifs fondamentaux consistant à assurer un niveau équivalent de protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données dans l'ensemble de l'Union, il est nécessaire et approprié de fixer des règles en ce qui concerne le traitement des données à caractère personnel par les institutions, organes, et organismes de l'Union. Le présent règlement ne va pas au-delà de ce qui est nécessaire pour atteindre les objectifs poursuivis, conformément à l'article 5, paragraphe 4, du traité sur l'Union européenne.

- **Choix de l'instrument**

Le règlement est considéré comme l'instrument juridique approprié pour définir le cadre 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. Il assure aux personnes physiques des droits opposables, précise les obligations de traitement des données qui incombent aux responsables de ce traitement au sein des institutions, organes et organismes de l'Union. Il crée aussi 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, organes et organismes de l'Union.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

La Commission a procédé à des consultations des parties intéressées en 2010 et en 2011 et à une analyse d'impact dans le cadre de la préparation du train de mesures réformant la protection des données, fournissant des informations sur les modifications qu'il est proposé d'apporter au règlement (CE) n° 45/2001. Dans ce contexte, la Commission a également mené une enquête auprès des coordinateurs de la protection des données (CPD)[5].

En ce qui concerne l'application pratique du règlement (CE) n° 45/2001 par les institutions, organes et organismes de l'Union, des informations ont été collectées auprès du Contrôleur européen de la protection des données (CEPD), d'autres institutions, organes et organismes de l'Union, d'autres DG de la Commission et d'un sous-traitant externe. Un questionnaire a été envoyé au réseau des délégués à la protection des données (DPD)[6].

Les délégués à la protection des données provenant d'un certain nombre d'institutions, organes et organismes de l'Union ont organisé des ateliers sur la réforme du règlement n° 45/2001 le 9 juillet 2015, le 22 octobre 2015, le 19 janvier 2016 et le 15 mars 2016.

La Commission a décidé, en 2013, de réaliser une étude d'évaluation sur l'application, à ce jour, du règlement (CE) n° 45/2001, qui a été confiée à un sous-traitant externe. Les résultats finaux de l'étude d'évaluation (rapport final, cinq études de cas et analyse article par article) ont été présentés à la Commission le 8 juin 2015[7].

L'évaluation a montré que le système de gouvernance structuré autour des DPD et du CEPD est efficace. Elle a démontré que le partage des compétences entre les DPD et le CEPD est clair et équilibré, et qu'ils disposent dans chaque cas d'un éventail approprié de compétences. Toutefois, des difficultés pourraient résulter d'un manque de pouvoir imputable à un soutien insuffisant des DPD de la part de leur hiérarchie.

---

5 Voir http://ec.europa.eu/justice/data-protection/reform/index_en.htm

6 Voir le rapport général du Contrôleur européen de la protection des données sur l'«Évaluation du respect du règlement (CE) n° 45/2001 au sein des institutions et organes de l'UE ("Enquête 2013")» et l'«Avis n° 3/2015 "Une grande opportunité pour l'Europe: recommandations du CEPD relatives aux options de l'UE en matière de réforme de la protection des données".»

7 JUST/2013/FRAC/FW/0157/A4 dans le cadre du contrat-cadre multiple JUST/2011/EVAL/01 (RS 2013/05) - Étude d'évaluation sur le règlement (CE) n° 45/2001, par Ernst et Young, disponible à l'adresse http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51087

L'étude d'évaluation a indiqué que la mise en application du règlement (CE) n° 45/2001 pourrait être améliorée par le recours à des sanctions de la part du CEPD. Une utilisation accrue de ses pouvoirs de contrôle pourrait conduire à une meilleure application des règles en matière de protection des données. Cette étude a également conclu que les responsables du traitement des données devraient adopter une approche de gestion des risques et procéder à des évaluations de risques avant d'effectuer des opérations de traitement, afin de mieux mettre en œuvre les exigences en matière de sécurité et de conservation des données.

L'étude a également montré que les règles existantes figurant au chapitre IV du règlement (CE) n° 45/2001 sur le secteur des télécommunications sont obsolètes et qu'il est nécessaire d'aligner ce chapitre sur la directive «vie privée et communications électroniques». D'après l'étude d'évaluation, il convient également d'éclaircir certaines définitions clés du règlement (CE) n° 45/2001. Il s'agit notamment de l'identification des responsables du traitement des données dans les institutions, organes et organismes de l'Union, de la définition des destinataires et de l'extension de l'obligation de confidentialité à des sous-traitants externes.

L'étude d'évaluation a également souligné la nécessité de simplifier le régime des notifications et contrôles préalables afin d'accroître l'efficacité et de réduire la charge administrative.

L'évaluateur a effectué une enquête en ligne auprès de 64 institutions, organes et organismes de l'UE. 422 responsables du traitement des données, 73 délégués à la protection des données (DPD), 118 coordinateurs de la protection des données (CPD) et 109 correspondants informatiques ont répondu aux questions posées dans l'enquête. L'évaluateur a également mené une série d'entretiens avec les parties intéressées. Le 26 mars 2015, l'évaluateur et la Commission ont organisé un atelier final, auquel ont participé de nombreux responsables du traitement des données, DPD, CPD, correspondants informatiques et représentants du CEPD.

- **Obtention et utilisation d'expertise**

Voir la référence à l'étude d'évaluation dans le cadre du point précédent.

- **Analyse d'impact**

La présente proposition aura une incidence essentiellement sur les institutions, organes, et organismes de l'Union. Cela a été confirmé par les informations collectées auprès du CEPD, d'autres institutions, organes et organismes de l'Union, des DG de la Commission et du sous-traitant externe. Par ailleurs, l'impact des nouvelles obligations découlant du règlement (UE) 2016/679, sur lequel il convient d'aligner le présent règlement, a été évalué dans le contexte des travaux préparatoires pour ce dernier. Cela rend superflue toute analyse d'impact spécifique pour le présent règlement.

- **Réglementation affûtée et simplification**

Sans objet

- **Droits fondamentaux**

Le droit à la protection des données à caractère personnel est énoncé à l'article 8 de la charte des droits fondamentaux de l'Union européenne (ci-après dénommée la «charte»), à

l'article 16 du TFUE et à l'article 8 de la Convention européenne des droits de l'homme. Ainsi que l'a souligné la Cour de justice de l'Union européenne[8], le droit à la protection des données à caractère personnel n'apparaît pas comme une prérogative absolue, mais doit être pris en considération par rapport à sa fonction dans la société[9]. La protection des données est également étroitement liée au respect de la vie privée et familiale, protégé par l'article 7 de la charte.

La présente proposition définit des règles relatives 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.

D'autres droits fondamentaux consacrés par la charte et susceptibles d'être affectés sont les suivants: la liberté d'expression (article 11); le droit de propriété, et notamment la protection de la propriété intellectuelle (article 17, paragraphe 2); l'interdiction de toute discrimination fondée sur la race, les origines ethniques, les caractéristiques génétiques, la religion ou les convictions, les opinions politiques ou toute autre opinion, un handicap ou l'orientation sexuelle (article 21); les droits de l'enfant (article 24); le droit à un niveau élevé de protection de la santé humaine (article 35); le droit d'accès aux documents (article 42); et le droit à un recours effectif et à accéder à un tribunal impartial (article 47).

4. INCIDENCE BUDGÉTAIRE

Voir la fiche financière jointe en annexe.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

Sans objet

- **Documents explicatifs (pour les directives)**

Sans objet

CHAPITRE I - DISPOSITIONS GÉNÉRALES

L'article 1er définit l'objet du règlement et, comme l'article 1er du règlement (CE) n° 45/2001, précise les deux objectifs poursuivis: protéger le droit fondamental à la protection des données et garantir la libre circulation des données à caractère personnel au sein de l'Union. Il présente également les principales missions du Contrôleur européen de la protection des données.

L'article 2 délimite le champ d'application du règlement: il s'applique au traitement de données à caractère personnel, effectué à l'aide de procédés automatisés ou d'une autre

[8] CJUE, arrêt du 9 novembre 2010, Volker und Markus Schecke et Eifert, affaires jointes C-92/09 et C-93/09, ECLI:EU:C:2009:284, point 48.

[9] Conformément à l'article 52, paragraphe 1, de la charte, des limitations peuvent être apportées à l'exercice du droit à la protection des données, dans la mesure où elles sont prévues par la loi, respectent le contenu essentiel du droit et des libertés en cause et, dans le respect du principe de proportionnalité, sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou au besoin de protection des droits et libertés d'autrui.

manière, par toutes les institutions et tous les organes de l'Union, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit de l'Union. Le champ d'application matériel de ce règlement est neutre sur le plan technologique. La protection des données à caractère personnel s'applique aux traitements de données à caractère personnel à l'aide de procédés automatisés ainsi qu'aux traitements manuels, si les données à caractère personnel sont contenues ou destinées à être contenues dans un fichier.

L'article 3 définit des termes employés dans le règlement. Outre les définitions des «institutions et organes de l'Union», du «responsable du traitement», de l'«utilisateur» et du «répertoire», qui sont spécifiques au présent règlement, les termes utilisés dans le présent règlement sont définis dans le règlement (UE) 2016/679, le règlement (UE) 0000/00 [nouveau règlement «vie privée et communications électroniques»], la directive 00/0000/UE [directive établissant le code des communications électroniques européen] et la directive 2008/63/CE de la Commission.

CHAPITRE II - PRINCIPES

L'article 4 énonce les principes relatifs au traitement des données à caractère personnel, qui correspondent à ceux définis à l'article 5 du règlement (UE) 2016/679. Par rapport au règlement (CE) n° 45/2001, il ajoute les nouveaux principes de la transparence et de l'intégrité et la confidentialité.

L'article 5 est fondé sur l'article 6 du règlement (UE) 2016/679 et fixe les critères de licéité du traitement, à la seule exception du critère des intérêts légitimes poursuivis par le responsable du traitement qui n'est pas applicable au secteur public et, dès lors, ne devrait pas s'appliquer aux institutions et organes de l'Union. L'article 5 maintient les critères déjà fixés au titre de l'article 5 du règlement (CE) n° 45/2001.

L'article 6 précise les conditions de traitement à une autre fin compatible conformément à l'article 6, paragraphe 4, du règlement (UE) 2016/679. Par rapport à l'article 6 du règlement (CE) n° 45/2001, cette nouvelle disposition permet une plus grande flexibilité et une plus grande sécurité juridique en ce qui concerne le traitement ultérieur à des fins compatibles.

L'article 7 précise, en accord avec l'article 7 du règlement (UE) 2016/679, les conditions dans lesquelles le consentement peut valablement fonder un traitement licite.

L'article 8 fixe, conformément à l'article 8 du règlement (UE) 2016/679, d'autres conditions de licéité pour le traitement des données à caractère personnel relatives aux enfants, en ce qui concerne l'offre directe de services de la société de l'information proposés à ces derniers. Il fixe à 13 ans l'âge minimum de l'enfant pour un consentement valable.

L'article 9 définit, conformément à l'article 8 du règlement (CE) n° 45/2001, des règles prévoyant un niveau de protection spécifique relatif à la transmission de données à caractère personnel à des destinataires autres que les institutions et organes de l'Union, établis dans l'Union et soumis au règlement (UE) 2016/679 ou à la directive (UE) 2016/680. Il précise que, si le responsable du traitement est à l'origine de la transmission, il devrait démontrer la nécessité et la proportionnalité de celle-ci.

L'article 10, qui s'inspire de l'article 9 du règlement (UE) 2016/679 et développe l'article 10 du règlement (CE) n° 45/2001, prévoit une interdiction générale des traitements portant sur

des catégories particulières de données à caractère personnel, et les exceptions à cette règle générale.

L'article 11 définit, conformément à l'article 10 du règlement (UE) 2016/679 et en accord avec l'article 10, paragraphe 5, du règlement (CE) n° 45/2001, les conditions de traitement des données à caractère personnel relatives à des condamnations et à des infractions pénales.

L'article 12 précise les informations que le responsable du traitement est tenu de fournir à la personne concernée, conformément à l'article 11 du règlement (UE) 2016/679, indiquant que 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'article 13 définit, sur la base de l'article 89, paragraphe 1, du règlement (UE) 2016/679, les règles concernant les 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.

CHAPITRE III - DROITS DE LA PERSONNE CONCERNÉE

Section 1 – Transparence et modalités

L'article 14 introduit, sur la base de l'article 12 du règlement (UE) 2016/679, l'obligation pour les responsables du traitement de fournir des informations transparentes, aisément accessibles et compréhensibles, et de prévoir des procédures et des mécanismes permettant à la personne concernée d'exercer ses droits, y compris, le cas échéant, les moyens d'effectuer une demande par voie électronique, la fixation d'un délai de réponse à la demande de la personne concernée et la motivation des refus. Étant donné que les institutions et organes de l'Union ne devraient en aucun cas exiger le paiement de frais liés aux coûts administratifs supportés pour fournir les informations, cette possibilité n'a pas été reprise du règlement (UE) 2016/679.

Section 2 - Information et accès aux données

Sur la base de l'article 13 du règlement (UE) 2016/679 et précisant l'article 11 du règlement (CE) n° 45/2001, l'article 15 définit les obligations d'information du responsable du traitement à l'égard de la personne concernée lorsque des données à caractère personnel sont collectées auprès de cette dernière, à savoir communiquer des informations à la personne concernée, notamment en ce qui concerne la durée de conservation des données, le droit d'introduire une réclamation et les transmissions internationales.

Se fondant sur l'article 14 du règlement (UE) 2016/679 et développant l'article 12 du règlement (CE) n° 45/2001, l'article 16 précise en outre que le responsable du traitement est tenu de fournir à la personne concernée, lorsque les données à caractère personnel n'ont pas été collectées auprès de cette dernière, des informations relatives à la source dont proviennent les données. Il reprend également les dérogations prévues dans le règlement (UE) 2016/679, à savoir que cette obligation d'information ne s'applique pas si la personne concernée dispose déjà de ces informations, si la fourniture de ces informations se révèle impossible ou exigerait des efforts disproportionnés pour le responsable du traitement, si les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou si l'enregistrement ou la communication des données à

caractère personnel sont expressément prévus par la loi. Cela pourrait, par exemple, s'appliquer aux procédures engagées par des services compétents en matière de santé ou de sécurité sociale.

L'article 17 prévoit, conformément à l'article 15 du règlement (UE) 2016/679 et développant l'article 13 du règlement (CE) n° 45/2001, des dispositions relatives au droit d'accès de la personne concernée aux données à caractère personnel la concernant, et ajoute de nouveaux éléments tels que l'obligation d'informer les personnes concernées de la durée de conservation, ainsi que de leurs droits à la rectification et à l'effacement des données et de leur droit d'introduire une réclamation.

Section 3 – Rectification et effacement

L'article 18 définit le droit de la personne concernée à la rectification, sur la base de l'article 16 du règlement (UE) 2016/679 et précisant l'article 14 du règlement (CE) n° 45/2001.

L'article 19 définit, conformément à l'article 17 du règlement (UE) 2016/679 et développant l'article 16 du règlement (CE) n° 45/2001, le droit de la personne concernée à l'oubli et à l'effacement des données personnelles la concernant. Il fixe les conditions du droit à l'oubli numérique, notamment l'obligation qui est faite au responsable du traitement ayant rendu publiques des données à caractère personnel d'informer les tiers de la demande de la personne concernée d'effacer tout lien vers ces données ou toute copie ou reproduction de celles-ci.

L'article 20 instaure le droit à la limitation du traitement dans certains cas, en évitant le terme équivoque de «verrouillage» utilisé dans le règlement (CE) n° 45/2001 et en assurant la cohérence avec la nouvelle terminologie introduite à l'article 18 du règlement (UE) 2016/679.

L'article 21 prévoit, en conformité avec l'article 19 du règlement (UE) 2016/679 et développant l'article 17 du règlement (CE) n° 45/2001, l'obligation faite au responsable du traitement de notifier 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, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit également à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.

L'article 22 introduit, conformément à l'article 20 du règlement (UE) 2016/679, le droit des personnes concernées à la portabilité des données, c'est-à-dire le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement ou d'obtenir que ces données soient transmises directement à un autre responsable du traitement, lorsque cela est techniquement possible. À titre de condition préalable et pour améliorer encore l'accès des personnes physiques aux données à caractère personnel les concernant, l'article prévoit le droit d'obtenir ces données du responsable du traitement dans un format structuré, couramment utilisé et lisible par machine. Ce droit s'applique uniquement lorsque le traitement est fondé sur le consentement de la personne concernée ou sur un contrat conclu par cette dernière.

Section 4 - Droit d'opposition et prise de décision individuelle automatisée

L'article 23 confère à la personne concernée un droit d'opposition sur la base de l'article 21 du règlement (UE) 2016/679 et précisant l'article 18 du règlement (CE) n° 45/2001.

L’article 24 porte sur le droit de la personne de ne pas faire l’objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, conformément à l’article 22 du règlement (UE) 2016/679 et précisant l’article 19 du règlement (CE) n° 45/2001.

Section 5 – Limitations

L’article 25 prévoit des limitations aux droits de la personne concernée visés aux articles 14 à 22 et aux articles 34 et 38 ainsi qu’aux principes fixés à l’article 4 (dans la mesure où les dispositions correspondent aux droits et obligations visés aux articles 14 à 22). De telles limitations devraient être fixées dans des actes juridiques adoptés sur la base des traités ou des règles internes des institutions et organes de l’Union. Si la possibilité d’une telle limitation n’est pas prévue dans les actes juridiques adoptés sur la base des traités ou des règles internes des institutions et organes de l’Union, ces derniers pourraient imposer une limitation ad hoc à condition qu’elle respecte l’essence des libertés et droits fondamentaux, dans le cadre d’un traitement spécifique, et constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir un ou plusieurs des objectifs autorisant des limitations applicables aux droits des personnes concernées. Cette approche est conforme à l’article 23 du règlement (UE) 2016/679. Cependant, contrairement à l’article 23 du règlement (UE) 2016/679 et conformément à l’article 20 du règlement (CE) n° 45/2001, cette disposition ne prévoit pas la possibilité de limiter le droit d’opposition de la personne concernée et le droit de la personne concernée de ne pas être soumise à une décision prise sur le seul fondement d'un traitement automatisé de données. Les exigences applicables aux limitations sont conformes à la charte des droits fondamentaux et à la Convention européenne des droits de l’homme, telles qu’interprétées par la Cour de justice de l’Union européenne et la Cour européenne des droits de l’homme, respectivement.

CHAPITRE IV — RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT

Section 1 — Obligations générales

L’article 26 s’inspire de l’article 24 du règlement (UE) 2016/679 et introduit le «principe de responsabilité» en décrivant les obligations incombant au responsable du traitement pour se conformer au présent règlement et démontrer qu’il le respecte, notamment par l’adoption de mesures techniques et organisationnelles appropriées et, le cas échéant, de politiques internes et de mécanismes destinés à assurer ce respect. L’article 24, paragraphe 3, du règlement (UE) 2016/679 n’a pas été conservé dans cette disposition, étant donné que les institutions et organes de l’Union ne sont pas tenus de se conformer à des codes de conduite ou des mécanismes de certification.

L'article 27 définit, conformément à l’article 25 du règlement (UE) 2016/679, les obligations du responsable du traitement qui découlent des principes de protection des données dès la conception et par défaut.

L’article 28 relatif aux responsables conjoints du traitement se fonde sur l’article 26 du règlement (UE) 2016/679 afin de préciser les responsabilités des responsables conjoints du traitement, qu’il s’agisse d’institutions ou organes de l’Union ou non, en ce qui concerne leurs relations internes et à l’égard de la personne concernée. Cette disposition règle la situation où tous les responsables conjoints du traitement sont couverts par le même régime juridique (le présent règlement) et les situations dans lesquelles certains sont couverts par le présent règlement et d’autres par un autre instrument juridique [le règlement (UE) 2016/679, la

directive (UE) 2016/680, la directive (UE) 2016/681 et d'autres régimes particuliers de protection des données concernant les institutions ou organes de l'Union].

L'article 29, qui s'inspire de l'article 28 du règlement (UE) 2016/679 et développe l'article 23 du règlement (CE) n° 45/2001, précise la fonction et les obligations des sous-traitants, et définit notamment que si, en violation du 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.

L'article 30 relatif au traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant est fondé sur l'article 29 du règlement (UE) 2016/679 et prévoit une interdiction pour le sous-traitant ou 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, de traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou d'un État membre.

L'article 31 s'appuie sur l'article 30 du règlement (UE) 2016/679 et introduit l'obligation, pour les responsables du traitement et les sous-traitants, de conserver une trace documentaire des opérations de traitement sous leur responsabilité, au lieu de la notification préalable au CEPD exigée par l'article 25 du règlement (CE) n° 45/2001 et l'inscription au registre des DPD. Contrairement au règlement (UE) 2016/679, cette disposition ne fait pas référence à des représentants, étant donné que les institutions de l'Union n'auront pas de représentants et auront toujours des délégués à la protection des données. Les références faites à des transferts sur la base de dérogations pour des situations particulières, comme dans le règlement (UE) 2016/679, n'ont pas été conservées, étant donné que ces types de transferts ne sont pas prévus dans le présent règlement. L'obligation de tenir un registre des activités de traitement effectuées peut être centralisée au niveau d'une institution ou d'un organe de l'Union. Dans ce cas, les institutions et organes de l'Union ont la possibilité de maintenir leur système de registres pour les activités de traitement sous la forme d'un registre accessible au public.

L'article 32 précise, sur la base de l'article 31 du règlement (UE) 2016/679, les obligations des institutions et organes de l'Union pour la coopération avec le CEPD.

Section 2 – Sécurité des données à caractère personnel et confidentialité des communications électroniques

L'article 33 oblige, dans le respect des dispositions de l'article 32 du règlement (UE) 2016/679 et développant celles de l'article 22 du règlement (CE) n° 45/2001, le responsable du traitement à mettre en œuvre les mesures appropriées pour garantir la sécurité du traitement. Il étend cette obligation aux sous-traitants, indépendamment du contrat conclu avec le responsable du traitement.

L'article 34 s'inspire de l'article 36 du règlement (CE) n° 45/2001 et garantit la confidentialité des communications électroniques effectuées au sein des institutions et organes de l'Union.

L'article 35 s'appuie sur la pratique actuelle des institutions et organes de l'Union et protège les informations relatives aux équipements terminaux des utilisateurs finals qui accèdent à leurs sites web et applications mobiles publics conformément au règlement (UE) XXXX/XX [nouveau règlement «vie privée et communications électroniques»], et notamment à son article 8.

L'article 36 s'inspire de l'article 38 du règlement (CE) n° 45/2001 et protège les données à caractère personnel contenues dans les annuaires publics et privés des institutions et organes de l'Union.

Les articles 37 et 38 introduisent une obligation de notification des violations de données à caractère personnel, conformément aux articles 33 et 34 du règlement (UE) 2016/679.

Section 3 – Analyse d'impact relative à la protection des données et consultation préalable

L'article 39 s'inspire de l'article 35 du règlement (UE) 2016/679 et introduit l'obligation, pour les responsables du traitement et les sous-traitants, d'effectuer une analyse d'impact relative à la protection des données préalablement aux opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Cette obligation s'applique en particulier dans le cas de l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, le traitement à grande échelle de catégories particulières de données ou la surveillance systématique à grande échelle d'une zone accessible au public.

L'article 40 est fondé sur l'article 36 du règlement (UE) 2016/679 et concerne les cas dans lesquels il est obligatoire d'obtenir l'autorisation du CEPD et de le consulter préalablement au traitement. Toutefois, le premier paragraphe de l'article 40 reprend le considérant 94 du règlement (UE) 2016/679 et vise à clarifier la portée de l'obligation de consultation.

Section 4 - Information et consultation législative

L'article 41 prévoit l'obligation pour les institutions et organes de l'Union d'informer le CEPD lorsqu'ils élaborent des mesures administratives et des règles internes relatives au traitement de données à caractère personnel.

L'article 42 prévoit l'obligation pour la Commission de consulter le CEPD après l'adoption de propositions d'acte législatif et de recommandations ou de propositions au Conseil conformément à l'article 218 du TFUE et lors de l'élaboration d'actes délégués ou d'actes d'exécution ayant une incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel. Lorsque ces actes revêtent 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 aussi consulter le comité européen de la protection des données. Dans ce cas, les deux entités devraient coordonner leurs travaux en vue de formuler un avis conjoint. Un délai de huit semaines pour la délivrance des avis dans les cas susmentionnés est établi, avec des dérogations possibles pour les cas d'urgence ou s'il y a autrement lieu, par exemple lorsque la Commission élabore des actes délégués et des actes d'exécution.

Section 5 – Obligation de répondre aux allégations

L'article 43 établit l'obligation, pour les responsables du traitement et le sous-traitant, de répondre aux allégations lorsque le CEPD a décidé de leur soumettre une question.

Section 6 – Délégué à la protection des données

L'article 44 s'appuie sur l'article 37, paragraphe 1, point a), du règlement (UE) 2016/679 et sur l'article 24 du règlement (CE) n° 45/2001 et prévoit la désignation d'un DPD obligatoire pour les institutions et organes de l'Union.

L’article 45 s’appuie sur l’article 38 du règlement (UE) 2016/679 et sur l’article 24 du règlement (CE) n° 45/2001 pour définir la fonction du délégué à la protection des données.

L’article 46 s’appuie sur l’article 39 du règlement (UE) 2016/679 ainsi que sur l’article 24 et les deuxième et troisième paragraphes de l’annexe au règlement (CE) n° 45/2001 pour définir les missions principales du délégué à la protection des données.

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

L’article 47 s’inspire de l’article 9 du règlement (CE) n° 45/2001 et énonce le principe général, conformément à l’article 44 du règlement (UE) 2016/679, selon lequel le respect d’autres dispositions du présent règlement et des conditions énoncées dans le chapitre V est obligatoire pour tout transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, 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.

L’article 48 prévoit qu’un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a décidé, conformément à l’article 45, paragraphe 3, du règlement (UE) 2016/679, qu’un niveau de protection adéquat est assuré dans le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou dans l’organisation internationale et que ce transfert vise exclusivement à permettre l’exécution des missions qui relèvent de la compétence du responsable du traitement. Les paragraphes 2 et 3 de cet article ont été repris de l’article 9 du règlement (CE) n° 45/2001, étant donné qu’ils sont des éléments utiles pour le suivi du niveau de protection dans les pays tiers et les organisations internationales.

L’article 49 s’appuie sur l’article 46 du règlement (UE) 2016/679 et subordonne les transferts vers des pays tiers pour lesquels la Commission n’a pas adopté de décision d'adéquation à la présentation de garanties appropriées, notamment des clauses types de protection des données et des clauses contractuelles. Des règles d’entreprise contraignantes, des codes de conduite et des mécanismes de certification pourraient être utilisés, en conformité avec le règlement (UE) 2016/679, par les responsables du traitement autres que les institutions et organes de l’Union. Le quatrième paragraphe de cet article sur l’obligation pour les institutions et organes de l’Union d’informer le CEPD des catégories de cas dans lesquels ils ont appliqué cet article correspond à l’article 9, paragraphe 8, du règlement (CE) n° 45/2001 et est maintenu en raison de sa spécificité. Le cinquième paragraphe s’appuie sur le maintien des autorisations existantes prévues à l’article 46, paragraphe 5, du règlement (UE) 2016/679.

L’article 50 précise, en accord avec l’article 48 du règlement (UE) 2016/679, que toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant le transfert ou la divulgation 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.

L’article 51 s’inspire de l’article 49 du règlement (UE) 2016/679 et définit et précise les dérogations pour un transfert de données. Cette disposition s'applique en particulier aux transferts de données qui sont nécessaires pour des motifs importants d'intérêt général, par exemple en cas de transfert international de données entre autorités de la concurrence,

administrations fiscales ou douanières, ou entre services chargés des questions de sécurité sociale ou de la gestion des activités de pêche. Le cinquième paragraphe sur l'obligation d'informer le CEPD des catégories de cas dans lesquels des dérogations ont été invoquées pour un transfert correspond à l'actuel article 9, paragraphe 8, du règlement (CE) n° 45/2001.

L'article 52 est fondé sur l'article 50 du règlement (UE) 2016/679 et prévoit explicitement des mécanismes de coopération internationale dans le domaine de la protection des données à caractère personnel entre le CEPD, en coopération avec la Commission et le comité européen de la protection des données, et les autorités de contrôle de pays tiers.

CHAPITRE VI - LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

L'article 53 s'appuie sur l'article 41 du règlement (CE) n° 45/2001 et concerne la mise en place du CEPD.

L'article 54, qui s'inspire de l'article 42 du règlement (CE) n° 45/2001 et de l'article 3 de la décision 1247/2002/CE, établit les règles pour la nomination du CEPD par le Parlement européen et le Conseil. Il précise également la durée de son mandat: cinq ans.

L'article 55, qui s'inspire de l'article 43 du règlement (CE) n° 45/2001 et de l'article 1er de la décision 1247/2002/CE, établit le statut et les conditions générales d'exercice des fonctions de CEPD et traite de ses ressources humaines et financières.

L'article 56 s'inspire de l'article 52 du règlement (UE) 2016/679 et de l'article 44 du règlement (CE) n° 45/2001 et clarifie les conditions garantissant l'indépendance du CEPD, en tenant compte de la jurisprudence de la Cour de justice de l'Union européenne.

L'article 57 définit, sur la base de l'article 45 du règlement (CE) n° 45/2001, les obligations de secret professionnel du CEPD pendant la durée de son mandat et après la cessation de celui-ci en ce qui concerne les informations confidentielles dont il a eu connaissance dans le cadre de l'exercice de ses fonctions.

L'article 58 se fonde sur l'article 57 du règlement (UE) 2016/679 et sur l'article 46 du règlement (CE) n° 45/2001, et définit les missions du CEPD, consistant notamment à recevoir et à examiner les réclamations, et à sensibiliser le public aux risques, règles, garanties et droits existants.

L'article 59 s'appuie sur l'article 58 du règlement (UE) 2016/679 et sur l'article 47 du règlement (CE) n° 45/2001 pour définir les pouvoirs du CEPD.

L'article 60 s'appuie sur l'article 59 du règlement (UE) 2016/679 et sur l'article 48 du règlement (CE) n° 45/2001 pour définir l'obligation pour le CEPD d'établir un rapport annuel d'activité.

CHAPITRE VII - COOPÉRATION ET COHÉRENCE

L'article 61 s'appuie sur l'article 61 du règlement (UE) 2016/679 et sur l'article 46, point f), du règlement (CE) n° 45/2001 pour introduire des règles explicites relatives à la coopération du CEPD avec les autorités de contrôle nationales.

L'article 62 énonce les obligations du CEPD dans les cas où d'autres actes de l'Union renvoient à cet article dans le cadre d'un contrôle coordonné avec les autorités de contrôle

nationales. Il vise à mettre en œuvre un modèle unique de contrôle coordonné. Ce modèle pourrait être utilisé pour assurer un contrôle coordonné des systèmes d'information à grande échelle tels qu'Eurodac, le système d'information Schengen II, le système d'information sur les visas, le système d'information douanier ou le système d'information du marché intérieur, mais aussi pour le contrôle de certaines agences de l'Union lorsqu'un modèle spécifique de coopération entre le CEPD et les autorités nationales a été établi, comme Europol. Le comité européen de la protection des données devrait constituer une enceinte unique pour assurer l'efficacité du contrôle coordonné à tous les niveaux.

CHAPITRE VIII – VOIES DE RECOURS, RESPONSABILITÉ ET SANCTIONS

L'article 63 s'appuie sur l'article 77 du règlement (UE) 2016/679 et sur l'article 32 du règlement (CE) n° 45/2001 et prévoit le droit pour toute personne concernée d'introduire une réclamation auprès du CEPD. Il établit également l'obligation pour le CEPD de traiter la réclamation et d'informer la personne concernée de l'état d'avancement et de l'issue de ladite réclamation dans un délai de trois mois, après lequel la plainte est réputée rejetée.

L'article 64 maintient l'article 32, paragraphe 1, du règlement (CE) n° 45/2001, précisant que la Cour de justice de l'Union européenne est compétente pour connaître de tout litige relatif aux dispositions du présent règlement, y compris les demandes de réparation.

L'article 65 établit le droit d'obtenir réparation pour tout dommage matériel ou préjudice moral subi, sous réserve des conditions prévues dans les traités, y compris en matière de responsabilité.

L'article 66 se fonde sur l'article 83 du règlement (UE) 2016/679 et prévoit la possibilité pour le CEPD d'infliger des amendes administratives aux institutions et organes de l'Union, en tant que sanction de dernier recours et uniquement lorsqu'une institution ou un organe de l'Union n'obtempère pas à un ordre du CEPD conformément aux points d) à h) et j) de l'article 59, paragraphe 2. L'article précise également les critères pour décider du montant de l'amende administrative, dans chaque cas d'espèce, et les plafonds annuels maximums s'inspirent des montants des amendes applicables dans certains États membres.

L'article 67 autorise, conformément à l'article 80, paragraphe 1, du règlement (UE) 2016/679, certains organismes, organisations ou associations à introduire une réclamation au nom de la personne concernée.

L'article 68 établit, conformément à l'article 33 du règlement (CE) n° 45/2001, des règles spécifiques visant à protéger le personnel de l'Union introduisant auprès du CEPD une réclamation pour une violation alléguée des dispositions du présent règlement, sans passer par les voies officielles.

L'article 69 s'inspire de l'article 49 du règlement (CE) n° 45/2001 et prévoit les sanctions applicables en cas de manquement aux obligations énoncées dans le présent règlement commis par des fonctionnaires ou autres agents de l'Union européenne.

CHAPITRE IX - ACTES D'EXÉCUTION

L'article 70 contient la disposition relative à la procédure de comité nécessaire pour conférer des compétences d'exécution à la Commission, dans les cas où, conformément à l'article 291

du TFUE, des conditions uniformes d'exécution d'actes juridiquement contraignants de l'Union sont nécessaires. La procédure d'examen s'applique.

CHAPITRE X - DISPOSITIONS FINALES

L'article 71 abroge le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE, et prévoit que les références aux deux instruments abrogés s'entendent comme faites au présent règlement.

L'article 72 précise que le présent règlement ne porte pas atteinte aux mandats actuels du Contrôleur européen de la protection des données et du contrôleur adjoint, et que l'article 54, paragraphes 4, 5 et 7, et les articles 56 et 57 du présent règlement s'appliquent à l'actuel contrôleur adjoint jusqu'à la fin de son mandat, le 5 décembre 2019.

L'article 73 fixe au 25 mai 2018 la date d'entrée en vigueur du présent règlement afin d'assurer la cohérence par rapport à la date d'application du règlement (UE) 2016/679.

2017/0002 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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

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[10],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

1) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après dénommée la «charte») et l'article 16,

[10] JO C du , p. .

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.

2) Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil[11] donne aux personnes physiques des droits juridiquement protégés, définit les obligations des responsables du traitement au sein des institutions et organes de l'Union 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[12] et la directive (UE) 2016/680 du Parlement européen et du Conseil[13] 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 souligne que pour mettre en place un cadre de protection des données solide et cohérent dans l'Union, il convient d'apporter les adaptations nécessaires au règlement (CE) n° 45/2001 de manière à ce que celles-ci s'appliquent en même temps que 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 et organes 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 se fondent sur la même notion que les dispositions du règlement (UE) 2016/679, les dispositions de ces deux instruments devraient être interprétées de manière homogène, notamment en raison du fait que le régime du présent règlement devrait être compris comme équivalent au régime du règlement (UE) 2016/679.

---

[11] 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).

[12] 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) (texte présentant de l'intérêt pour l'EEE) (JO L 119 du 4.5.2016, p. 1).

[13] 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).

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, sont susceptibles d'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 concernent les personnes morales, et en particulier des 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. Elle devrait s'appliquer aux traitements de données à caractère personnel à l'aide de procédés automatisés ainsi qu'aux traitements manuels, si les données à caractère personnel sont contenues ou destinées à être contenues dans un fichier. Les dossiers ou ensembles de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés ne devraient pas relever du champ d'application du présent règlement.

8) 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 TFUE pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines. Le présent règlement devrait donc s'appliquer aux agences de l'Union menant des activités dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière uniquement dans la mesure où la législation de l'Union applicable à de telles agences ne contient aucune règle spécifique relative au traitement des données à caractère personnel.

9) La directive (UE) 2016/680 devrait prévoir 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 agences de l'Union menant des activités dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière et les autorités compétentes des États membres, les règles pour la protection et la libre circulation des données opérationnelles à caractère personnel traitées par ces agences de l'Union devraient s'inspirer des principes sous-tendant le présent règlement et être cohérentes avec la directive (UE) 2016/680.

10) Lorsque l'acte fondateur d'une agence de l'Union menant des activités relevant des chapitres 4 et 5 du titre V du traité établit un régime autonome de protection des données pour le traitement des données opérationnelles à caractère personnel, il convient que ce régime ne soit pas affecté par le présent règlement. Toutefois, conformément à l'article 62 de la directive (UE) 2016/680, la Commission devrait, au plus tard le 6 mai 2019, réexaminer les actes juridiques adoptés par l'Union qui

réglementent le traitement 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et formuler, le cas échéant, les propositions nécessaires en vue de modifier ces actes pour assurer une approche cohérente de la protection des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière.

11) 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 aux 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 ne soit pas ou 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.

12) 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.

13) 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.

14) 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.

15) 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 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, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement.

16) Conformément au principe de responsabilité, lorsque des institutions et organes de l'Union se transmettent des données à caractère personnel ou les transmettent en interne, ils devraient vérifier si ces données à caractère personnel sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire si celui-ci n'est pas un responsable du traitement. 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, et il devrait procéder à une évaluation provisoire de la nécessité du transfert 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.

17) 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 leur autorité publique, sur la nécessité de respecter l'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 ou 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 nécessaires 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 à la sauvegarde des intérêts vitaux de la personne concernée ou 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.

18) Le droit de l'Union incluant les règles internes visées dans le présent règlement devrait être clair et précis et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme.

19) 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; la nature des données à caractère personnel; les conséquences pour les personnes concernées du traitement ultérieur prévu; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu.

20) 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[14], 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.

21) 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 lors de l'utilisation de services proposés directement à un enfant sur des sites web d'institutions et organes de l'Union, comme les services de communication interpersonnels ou la vente en ligne de tickets et lorsque le traitement des données à caractère personnel repose sur le consentement.

22) Lorsque des destinataires établis dans l'Union et soumis au règlement (UE) 2016/679 ou à la directive (UE) 2016/680 souhaiteraient que des données à caractère personnel leur soient transmises par des institutions et organes de l'Union, ces destinataires devraient démontrer que la transmission est nécessaire à la réalisation de leur objectif, qu'elle est proportionnée et qu'elle ne va pas au-delà de ce qui est nécessaire pour atteindre cet objectif. Les institutions et organes de l'Union devraient démontrer cette nécessité lorsqu'ils sont eux-mêmes à l'origine de la transmission, conformément au principe de transparence.

23) 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. 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

[14] 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).

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 objet de permettre l'exercice des libertés fondamentales.

24) 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[15], 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 par des tiers.

25) 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 utilisés par la personne concernée pour se connecter au service en ligne proposé par le responsable du traitement.

26) 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

[15] 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).

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 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 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.

27) 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.

28) 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.

29) 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.

30) 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.

31) 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 important, 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.

32) Afin de renforcer le «droit à l'oubli» numérique, le droit à l'effacement devrait également être étendu de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques soit tenu d'informer les responsables du

traitement qui traitent 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.

33) 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 à ce que les données à caractère personnel ne fassent pas l'objet d'opérations de traitements 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.

34) Pour renforcer encore le contrôle qu'elles exercent sur leurs propres données, il convient de conférer aussi aux personnes concernées 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 prévues par 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.

35) 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 un 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.

36) 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'elle produit des effets juridiques concernant la personne en question ou qu'elle 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 risques d'erreur soit réduit au minimum, et 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 qui prévienne, entre autres, les effets discriminatoires à l'égard des personnes physiques fondées sur la 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 qui se traduisent par des mesures produisant un tel effet. La prise de décision et le profilage automatisés fondés sur des catégories particulières de données à caractère personnel ne devraient être autorisés qu'à des conditions spécifiques.

37) 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 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 les actes juridiques adoptés sur la base des traités ou des règles internes des institutions et organes de l'Union, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité publique, la prévention 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, y compris la protection de la vie humaine, particulièrement en réponse à des catastrophes d'origine naturelle ou humaine, pour garantir 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, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, la tenue de registres publics conservés 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.

Si aucune limitation n'est prévue dans les actes juridiques adoptés sur la base des traités ou des règles internes des institutions et organes de l'Union, ces institutions et ces organes peuvent, dans un cas spécifique, imposer une limitation ad hoc à certains principes spécifiques ainsi qu'aux droits d'une personne concernée si cette limitation respecte l'essence des libertés et droits fondamentaux et, en ce qui concerne l'opération de traitement spécifique, si elle est nécessaire et proportionnée dans une société démocratique pour garantir un ou plusieurs des objectifs mentionnés au premier alinéa. La limitation devrait être notifiée au délégué à la protection des données. Il y a lieu que toutes les limitations respectent les exigences énoncées par la charte et par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

38) 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 l'étendue, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques. 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, ou 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. 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 l'étendue, 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.

39) 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.

40) La protection des droits et libertés des personnes concernées, de même que la responsabilité des responsables du traitement et de leurs sous-traitants, exige une répartition claire des responsabilités dans le cadre du présent règlement, notamment dans le cas où le responsable du traitement détermine les finalités et les moyens du traitement conjointement avec d'autres responsables, ou lorsqu'un traitement est effectué pour le compte d'un responsable du traitement.

41) Afin que les exigences du présent règlement soient respectées dans les cas où le traitement est 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 autre 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 devrait être régie par un contrat ou un autre acte juridique établi en vertu du droit de l'Union ou du droit d'un État membre, liant le sous-traitant au responsable du traitement, définissant l'objet et la durée du traitement, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées, 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.

42) 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. Les institutions et organes de l'Union devraient pouvoir établir un registre centralisant les registres de leurs activités de traitement. Pour des raisons de transparence, ils devraient aussi pouvoir rendre ce registre public.

43) 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, d'origine accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels, ou moraux.

44) 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, protéger les informations liées à l'équipement terminal des utilisateurs finaux ayant accès à leurs sites web et applications mobiles accessibles au public conformément au règlement (UE) XXXX/XX [nouveau règlement «vie privée et communications électroniques»] et protéger leurs données à caractère personnel dans les annuaires d'utilisateurs.

45) 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 moraux. En conséquence, dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il convient qu'il la notifie 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 conviendrait 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.

(46) Afin que la personne concernée puisse prendre les précautions qui s'imposent, il convient que le responsable du traitement lui communique toute violation de données à caractère personnel dans les meilleurs délais lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique. 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. De telles communications aux personnes concernées devraient être 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.

47) 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, qui, à son tour, tient un registre des opérations de traitement notifiées. Or, cette obligation génère une charge administrative et financière, sans pour autant avoir systématiquement contribué à améliorer la protection des données à caractère personnel. Ces obligations générales de notification sans distinction devraient dès lors être supprimées et remplacées par des procédures et des mécanismes efficaces ciblant plutôt les types d'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. Ces types d'opérations de traitement pourraient inclure ceux qui, notamment, 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.

48) 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, le Contrôleur européen de la protection des données devrait être consulté 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 un délai déterminé. Toutefois, l'absence de réaction du Contrôleur européen de la protection des données dans ce délai ne devrait pas empêcher une 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.

49) Le Contrôleur européen de la protection des données devrait être informé des mesures administratives et des règles internes des institutions et organes de l'Union qui 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 et, notamment, d'atténuer le risque encouru par la personne concernée.

50) 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 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 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 TFUE, 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 TFUE, 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 particuliers à l'égard du traitement de leurs données à caractère personnel, la Commission devrait pouvoir, en plus, 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.

51) Dans chaque institution ou organe 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 un niveau de 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 et de la protection exigée pour les données à caractère personnel traitées par le responsable du traitement ou le sous-traitant. Les délégués à la protection des données devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance.

52) Lorsque des données à caractère personnel sont transférées par les 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 ne devrait pas être compromis, y compris en cas de transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale à des responsables du traitement ou sous-traitants dans le même pays tiers ou dans un pays tiers différent, ou à une autre organisation internationale. En tout état de cause, les transferts vers des pays tiers et des organisations internationales ne peuvent avoir lieu que dans le plein respect du présent règlement. 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 pour le 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.

53) La Commission peut décider, en vertu de l'article 45 du règlement (UE) 2016/679, qu'un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale propose 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.

54) 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 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 conformément au règlement (UE) 2016/79. 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 de 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.

55) 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 au moyen d'engagements contractuels qui viendraient compléter les clauses types de protection des données.

56) 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.

57) 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.

58) 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.

59) 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 à ce que lesdites personnes continuent de bénéficier des droits fondamentaux et des garanties.

60) 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 au sein de l'Union, y compris le Contrôleur européen de la protection des données, peuvent être confrontées 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 elles disposent en matière de prévention ou de recours, par l'hétérogénéité des régimes juridiques et par des obstacles pratiques tels que le manque de ressources. Par conséquent, une coopération plus étroite entre le Contrôleur européen de la protection des données et d'autres autorités de contrôle de la protection des données devrait être encouragée afin de contribuer à l'échange d'informations avec leurs homologues internationaux.

61) La mise en place du Contrôleur européen de la protection des données dans le règlement n° 45/2001, 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.

62) 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 des États membres, ce qui inclut 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 de justice de l'Union européenne et d'ester en justice conformément au droit primaire. Ces pouvoirs devraient également inclure celui d'imposer une limitation temporaire ou définitive au traitement, et d'interdire ce dernier. 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 la conformité avec le 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.

63) 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.

64) 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 de ces données 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 celles 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.

65) 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. En outre, le Contrôleur européen de la protection des données est l'autorité de contrôle d'Europol et un modèle spécifique de coopération avec les autorités de contrôle nationales est mis en place dans le cadre d'un comité de coopération de nature 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, lorsqu'il y a lieu, soumettre des propositions législatives visant à modifier les actes juridiques 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 garantissant un contrôle coordonné efficace de manière systématique.

66) 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 de justice de l'Union européenne 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 suite à 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.

67) 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 le traité.

68) 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 infliger des amendes administratives en tant que sanction de dernier recours. Ces amendes devraient avoir pour objectif de sanctionner l'institution ou l'organe - 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 ainsi que les plafonds et critères pour fixer les amendes administratives 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 inflige une amende administrative à 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 en matière d'imposition d'amendes aux institutions et organes de l'Union devrait respecter les principes généraux du droit de l'Union tels qu'interprétés par la Cour de justice de l'Union européenne.

69) Lorsqu'une personne concernée estime que les droits que lui confère le présent règlement ne sont pas respectés, elle devrait avoir le droit de mandater un organisme, une organisation ou une association 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 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.

70) Un fonctionnaire ou autre agent de l'Union qui ne se conforme pas aux obligations lui incombant en vertu des dispositions du présent règlement s'expose à une sanction disciplinaire ou à toute autre action, conformément aux règles et procédures prévues dans le statut des fonctionnaires de l'Union européenne ou dans le régime applicable aux autres agents de l'Union européenne.

71) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission lorsque le présent règlement le prévoit. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil[16]. 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 lorsque les responsables du traitement procédant à un traitement nécessaire à l'exécution d'une mission d'intérêt public sont tenus de consulter le Contrôleur européen de la protection des données au préalable, et pour l'adoption de clauses contractuelles types mettant en place des garanties appropriées pour les transferts internationaux.

72) 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 TFUE. Le règlement (CE) n° 223/2009 du Parlement européen et du Conseil[17] contient d'autres dispositions particulières relatives aux statistiques européennes couvertes par le secret.

73) Il convient d'abroger le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE. Les références faites au règlement et à la décision abrogés devraient s'entendre comme faites au présent règlement.

74) 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

---

16 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).

17 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).

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.

75) 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 et la libre circulation des données à caractère personnel dans l'ensemble de l'Union, et à 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.

76) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001, et a rendu son avis le XX/XX/XXXX.

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, organes et organismes de l'Union, ainsi que des règles relatives à la libre circulation des données à caractère personnel entre ces institutions, organes et organismes ou vers des destinataires établis dans l'Union et soumis au règlement (UE) 2016/679[18] ou aux dispositions de droit interne adoptées en vertu de la directive (UE) 2016/680[19].

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.

[18] 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) (texte présentant de l'intérêt pour l'EEE) (JO L 119 du 4.5.2016, p. 1).

[19] 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).

3. Le Contrôleur européen de la protection des données (ci-après le «CEPD») veille à 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, dans la mesure où ce traitement est effectué pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit de l'Union.

2. 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

1. Aux fins du présent règlement, les définitions suivantes s'appliquent:

   (a) les définitions figurant dans le règlement (UE) 2016/679, à l'exception de la définition du terme «responsable du traitement» figurant à l'article 4, point 7), de ce règlement;

   (b) la définition du terme «communications électroniques» figurant à l'article 4, paragraphe 2, point a), du règlement (UE) XX/XXXX (règlement «vie privée et communications électroniques»);

   (c) les définitions des termes «réseau de communications électroniques» et «utilisateur final» figurant respectivement à l'article 2, point 1), et à l'article 2, point 14), de la directive 00/0000/UE [directive établissant le code des communications électroniques européen];

   (d) la définition du terme «équipement terminal» figurant à l'article 1er, point 1), de la directive 2008/63/CE de la Commission[20].

2. En outre, aux fins du présent règlement, on entend par:

   (e) «institutions et organes de l'Union»: les institutions, organes et organismes créés en vertu, ou sur la base, du traité sur l'Union européenne, du traité sur le fonctionnement de l'Union européenne ou du traité Euratom;

   (f) «responsable du traitement»: l'institution, organe ou organisme de l'Union, 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 du

[20] 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).

traitement sont déterminés par un acte spécifique de l'Union, le responsable du traitement ou les critères spécifiques applicables pour le désigner peuvent être fixés par le droit de l'Union;

(g) «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;

(h) «annuaire»: annuaire des utilisateurs accessible au public ou 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.

CHAPITRE II

PRINCIPES

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);

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 sur la base ou dans 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. La mission d'intérêt public mentionnée au paragraphe 1, point a), est inscrite 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 ni sur une disposition du droit de l'Union constituant une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs mentionnés 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 et à des infractions pénales 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 des enfants 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 13 ans. Lorsque l'enfant est âgé de moins de 13 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, autres que les institutions et organes de l'Union, établis dans l'Union et soumis au règlement (UE) 2016/679 ou à la directive (UE) 2016/680

1. Sans préjudice des articles 4, 5, 6 et 10, des données à caractère personnel ne sont transmises à des destinataires établis dans l'Union et soumis au règlement (UE) 2016/679 ou à la réglementation nationale adoptée en vertu de la directive (UE) 2016/680 que si le destinataire démontre:

   a) que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique, ou

   b) que la transmission des données est nécessaire et proportionnée à sa finalité et s'il n'existe aucune raison de penser que cette transmission pourrait porter atteinte aux droits, libertés et intérêts légitimes de la personne concernée.

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

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 pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union prévoit que l'interdiction mentionnée 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 lui des contacts réguliers en liaison avec ses objectifs et que les données ne soient pas divulguées à un tiers extérieur à 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 de justice de l'Union européenne agit dans le cadre de ses fonctions juridictionnelles;

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base de dispositions du droit de l'Union proportionnées à l'objectif poursuivi, respectant l'essence du droit à la protection des données et prévoyant 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 précisées 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 de dispositions du droit de l'Union qui prévoient des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel;

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 de dispositions du droit de l'Union proportionnées à l'objectif poursuivi, respectant l'essence du droit à la protection des données et prévoyant des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

3. Les données à caractère personnel mentionnées 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 sous la responsabilité d'un tel professionnel.

Article 11
Traitement de données à caractère personnel relatives à des condamnations et à des infractions pénales

Le traitement de données à caractère personnel relatives à des condamnations et à des infractions pénales ou à des mesures de sûreté connexes, conformément à l'article 5, paragraphe 1, ne peut être effectué que s'il est autorisé par le droit de l'Union, ce qui peut inclure des règles internes, prévoyant des garanties spécifiques et 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 mentionnés 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 cette dernière, 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 mentionnée aux articles 15 et 16 ainsi que pour procéder à toute communication au titre des articles 17 à 24 et de l'article 38 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 par les articles 17 à 24. Dans les cas mentionnés 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 sur le fondement 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 suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder, et au plus tard dans un délai d'un mois à compter de la réception de la demande, des motifs de son inaction et de la possibilité d'introduire une réclamation auprès 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 ni pour procéder à une communication ou prendre une mesure au titre des articles 17 à 24 et de l'article 38. 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. Si 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 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 de la Commission ou, dans le cas des transferts visés à l'article 49, 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 mentionnées 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 pendant laquelle les données à caractère personnel seront conservées 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 mentionnée 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 établi dans un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation de la Commission ou, dans le cas des transferts visés à l'article 49, 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 mentionnées 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 pendant laquelle les données à caractère personnel seront conservées 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 des données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues 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 mentionnées aux paragraphes 1 et 2:

(a) dans un délai raisonnable après l'obtention des données à caractère personnel, ce délai 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 elles 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 mentionnée 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 prévue 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; 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.

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 49, 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 prévu 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 mentionnée 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 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 prévu 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 des données à caractère personnel 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, excepté aux fins de leur 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 système de façon à ce qu'il apparaisse clairement que ces données 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 vertu 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, 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 prévu 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 prévu 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 34 et 35, 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 mentionnés 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 mentionnées au paragraphe 2 ne peuvent être fondées sur les catégories particulières de données à caractère personnel mentionnées 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 ou organes de l'Union, des règles internes fixées par ces derniers peuvent limiter l'application des articles 14 à 22 et des articles 34 et 38, 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, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;

(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 énumérés 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. Lorsqu'aucune limitation n'est prévue par un acte juridique adopté sur la base des traités ou par une règle interne conformément au paragraphe 1, les institutions et organes de l'Union peuvent limiter l'application des articles 14 à 22 et des articles 34 et 38, 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, en lien avec une opération de traitement spécifique, et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir un ou plusieurs des objectifs énumérés au paragraphe 1. La limitation est notifiée au délégué à la protection des données compétent.

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 les règles internes, peut prévoir des dérogations aux droits prévus aux articles 17, 18, 20 et 23, sous réserve des conditions et des garanties énumérées 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 les règles internes, peut prévoir des dérogations aux droits prévus aux articles 17, 18, 20, 21, 22 et 23, sous réserve des conditions et des garanties énumérées 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 mentionnées aux paragraphes 1, 3 et 4 sont suffisamment claires et précises et font l'objet d'une publication adéquate.

6. Si une limitation est imposée en vertu du paragraphe 1 ou 2, 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 ou 2 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 mentionnées aux paragraphes 6 et 7 et à l'article 46, paragraphe 2, peut être différée, omise ou refusée si elle annule l'effet de la limitation imposée en vertu du paragraphe 1 ou 2.

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 l'étendue, 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 faire en sorte que le traitement soit effectué conformément au présent règlement et être en mesure de le démontrer . Ces mesures sont réexaminées et actualisées si nécessaire.

2. Lorsque cela est proportionné au regard des activités de traitement, les mesures mentionnées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le 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 l'étendue, 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.

Article 28
Responsables conjoints du traitement

1. Lorsqu'une institution ou un organe de l'Union et un ou plusieurs responsables du traitement, qui peuvent être (ou non) des institutions ou 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 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 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 des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

3. La personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre un ou plusieurs des responsables du traitement, en tenant compte de leur rôle tel que défini dans les termes de l'accord mentionné au paragraphe 1.

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 pour 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 contre ces changements.

3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique établi en vertu 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 40, 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 mandaté par ce dernier, et contribuer à ces audits.

En ce qui concerne le point h) du premier alinéa, 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 établi en vertu 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 à ce 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 énumérées aux paragraphes 1 et 4 du présent article.

6. Sans préjudice d'un éventuel contrat particulier entre le responsable du traitement et le sous-traitant, le contrat ou l'autre acte juridique mentionné aux paragraphes 3 et 4 du présent article peut être fondé, en tout ou en partie, sur les clauses contractuelles types mentionnées 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 éléments énumérés aux paragraphes 3 et 4 du présent article et conformément à la procédure d'examen prévue à l'article 70, paragraphe 2.

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

9. Le contrat ou l'autre acte juridique mentionné aux paragraphes 3 et 4 se présente sous une forme écrite, y compris au format 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 et 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 traitent ces données que 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, s'il y a lieu, 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, des pays tiers ou des organisations internationales;

e) s'il y a lieu, 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 énumérées 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) s'il y a lieu, 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 énumérées à l'article 33.

3. Les registres prévus aux paragraphes 1 et 2 se présentent sous une forme écrite, y compris la 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. Les institutions et organes de l'Union peuvent décider de tenir leurs registres des activités de traitement dans un registre central. Dans ce cas, ils peuvent également décider de mettre 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 fonctions.

SECTION 2

SÉCURITÉ DES DONNÉES À CARACTÈRE PERSONNEL ET CONFIDENTIALITÉ DES COMMUNICATIONS ÉLECTRONIQUES

Article 33
Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de l'étendue, 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 destinées à assurer la sécurité du traitement.

2. Lors de l'évaluation du caractère approprié du niveau de sécurité, il est tenu compte en particulier des risques que présente le traitement, résultant notamment, de manière accidentelle ou illicite, 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.

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 que sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union.

Article 34
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 35
Protection des informations relatives aux équipements terminaux des utilisateurs finals

Les institutions et organes de l'Union protègent les informations relatives aux équipements terminaux des utilisateurs finals qui accèdent à leurs sites web et applications mobiles publics conformément au règlement (UE) XX/XXXX [nouveau règlement relatif à la vie privée et aux communications électroniques], et notamment son article 8.

Article 36
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.

Article 37
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 mentionnée 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, s'il y a lieu, 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 38
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 mentionnée au paragraphe 1 du présent article décrit la nature de la violation de données à caractère personnel en des termes clairs et simples et contient au moins les informations et mesures énumérées à l'article 37, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée mentionnée au paragraphe 1 n'est pas nécessaire si l'une 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 mentionné 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 énumérées au paragraphe 3 est remplie.

SECTION 3

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 l'étendue, 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 prévue 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 mentionnées 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. 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 mentionnés 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.

7. 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.

8. S'il y a lieu, 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.

9. Lorsque le traitement effectué en vertu 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 en préalable à l'adoption de l'acte juridique en question, les paragraphes 1 à 6 ne s'appliquent pas, à moins que le droit de l'Union n'en dispose autrement.

10. 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'il ressort d'une analyse d'impact relative à la protection des données effectuée en application de l'article 39 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 mentionné 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, s'il y a lieu, au sous-traitant, et peut faire usage des pouvoirs prévus à l'article 59. 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, s'il y a lieu, 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) s'il y a lieu, 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 voie d'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 effectué dans le cadre d'une mission d'intérêt public exercée par un responsable du traitement, y compris le traitement de données dans le cadre de la protection sociale et de la santé publique.

SECTION 4

INFORMATION ET CONSULTATION LÉGISLATIVE

Article 41
Information

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 impliquant une institution ou un organe de l'Union, seuls ou conjointement avec d'autres.

Article 42
Consultation législative

1. Après l'adoption de propositions d'acte législatif et de recommandations ou de propositions au Conseil en vertu de l'article 218 du TFUE et lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le Contrôleur européen de la protection des données lorsque ces propositions, recommandations ou actes ont une 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 mentionné 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 prévus aux paragraphes 1 et 2 sont communiqués par écrit dans un délai maximum 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) 2016/659 fait obligation à la Commission de consulter le comité européen de la protection des données.

SECTION 5

OBLIGATION DE RÉPONDRE AUX ALLÉGATIONS

Article 43
Obligation de répondre aux allégations

Lorsque le Contrôleur européen de la protection des données exerce les pouvoirs prévus à l'article 59, 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.

SECTION 6

DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Article 44
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 énumérées à l'article 46.

4. Le délégué à la protection des données peut être un membre du personnel de l'institution ou de l'organe de l'Union, ou exercer 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 45
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 énumérées à l'article 46 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 ses 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 directement, sans passer par les voies officielles, sur toute question concernant l'interprétation ou l'application du présent règlement, par le responsable du traitement et le sous-traitant, par le comité du personnel concerné ou encore par toute personne physique. 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 qu'avec le consentement du Contrôleur européen de la protection des données, s'il ne remplit plus les conditions requises pour l'exercice de ses fonctions.

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 46
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 et 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 37 et 38;

   (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 conformément à 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 conformément à l'article 40 et 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.

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 47
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 à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis.

Article 48
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, qu'un niveau de protection adéquat est assuré dans le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale et que ce transfert vise exclusivement à 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 que le pays tiers ou l'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, paragraphes 3 et 5, du règlement (UE) 2016/679, qu'un pays tiers ou une organisation internationale assure ou n'assure plus un niveau de protection adéquat.

Article 49
Transferts moyennant des garanties appropriées

1. En l'absence de décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679, 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 mentionnées 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 prévue à l'article 70, 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 prévue à l'article 70, paragraphe 2;

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

3. Sous réserve de l'autorisation du Contrôleur européen de la protection des données, les garanties appropriées mentionnées 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 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.

5. 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 ledit contrôleur.

Article 50
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 51
Dérogations pour des situations particulières

1. En l'absence de décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 ou de garanties appropriées conformément à l'article 49, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peuvent être effectués que si l'une des conditions suivantes est respectée:

   (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; ou

   (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 est effectué à partir d'un registre qui, conformément à la législation de l'Union, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, mais seulement dans la mesure où les conditions fixées par la législation de l'Union pour la consultation sont remplies dans le cas particulier.

2. Un transfert effectué en vertu du paragraphe 1, point g), ne porte pas sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre, 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.

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

4. 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.

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 52
Coopération internationale dans le domaine de la protection des données à caractère personnel

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

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Article 53
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 exerce les fonctions prévues à l'article 58 et les pouvoirs qui lui sont conférés à l'article 59.

Article 54
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 permettra 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. 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 pouvoir émettre une préférence.

2. La liste établie par la Commission, à partir de laquelle le Contrôleur européen de la protection des données est choisi, doit être constituée de personnes offrant toutes garanties d'indépendance et qui possèdent l'expérience et les compétences requises pour l'accomplissement des fonctions de Contrôleur européen de la protection des données, par exemple parce qu'ils appartiennent ou ont appartenu aux autorités de contrôle instituées en vertu de l'article 41 du règlement (UE) 2016/679.

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 remercié 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 de justice de l'Union européenne, 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 55
Statut et conditions générales d'exercice des fonctions 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 de justice de l'Union européenne 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'exécution de ses fonctions.

3. Le budget du Contrôleur européen de la protection des données figure sur une ligne spécifique de la section IX du budget général de l'Union européenne.

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.

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 européenne.

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

Article 56
Indépendance

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

2. Dans l'exercice de ses fonctions 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 57
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 58
Fonctions

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

   (a) contrôle et assure l'application du présent règlement et des autres actes de l'Union relatifs à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par une institution ou un organe de l'Union, à l'exclusion du traitement de données à caractère personnel par la Cour de justice de l'Union européenne 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 que leur impose le 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 des États membres;

(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, en particulier 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 toutes les institutions et tous les 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) surveille les faits nouveaux présentant un intérêt, dans la mesure où ils ont une incidence sur la protection des données à caractère personnel, notamment l'évolution des technologies de l'information et des communications;

(i) adopte les clauses contractuelles types mentionnées à l'article 29, paragraphe 8, et à l'article 49, paragraphe 2, point c);

(j) établit et tient à jour une liste ayant trait à 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 institué par l'article 68 du règlement (UE) 2016/679;

(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 mentionné à l'article 40, paragraphe 2;

(n) autorise les clauses contractuelles et les dispositions mentionnées à l'article 49, paragraphe 3;

(o) tient des registres internes des violations du présent règlement et des mesures prises conformément à l'article 59, paragraphe 2;

(p) s'acquitte de toute autre fonction 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 mentionnées 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'exercice des fonctions 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 59
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'exercice de ses fonctions;

   (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'exercice de ses fonctions;

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

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 vertu 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, si nécessaire, 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 vertu de l'article 19, paragraphe 2, et de l'article 21;

(i) imposer une amende administrative en vertu de l'article 66, dans l'hypothèse où l'institution ou l'organe de l'Union ne se conformerait pas aux mesures prévues au présent paragraphe et 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 prévue à l'article 40;

(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 mentionnées à l'article 29, paragraphe 8, et à l'article 49, paragraphe 2, point c);

(e) autoriser les clauses contractuelles mentionnées à l'article 49, paragraphe 3, point a);

(f) autoriser les arrangements administratifs mentionnés à l'article 49, paragraphe 3, point b);

4. 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.

5. Le Contrôleur européen de la protection des données a le pouvoir de saisir la Cour de justice de l'Union européenne dans les conditions prévues par le traité et d'intervenir dans les affaires portées devant la Cour de justice de justice de l'Union européenne.

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 d'activité 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 avec les autorités de contrôle nationales

Le Contrôleur européen de la protection des données coopère avec les autorités de contrôle instituées en vertu de l'article 41 du règlement (UE) 2016/679 et de l'article 51 de la directive (UE) 2016/680 (ci-après dénommées 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[21], dans la mesure nécessaire à l'exercice de leurs fonctions respectives, notamment en échangeant toute information utile, en demandant aux autorités nationales de contrôle d'exercer leurs pouvoirs ou en répondant aux demandes de ces autorités.

Article 62
Contrôle conjoint 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 doit coopérer activement avec les autorités de contrôle nationales, afin d'assurer un contrôle effectif des systèmes d'information à grande échelle ou des agences de l'Union.

2. Le Contrôleur européen de la protection des données, agissant dans le cadre de ses compétences et de ses responsabilités, doit échanger des informations utiles, aider à réaliser des audits et des inspections, examiner les difficultés d'interprétation ou d'application du présent règlement et d'autres actes de l'Union applicables, étudier les problèmes susceptibles de se présenter lors de l'exercice d'un contrôle indépendant ou lors de l'exercice des droits des personnes concernées, définir des propositions harmonisées visant à trouver des solutions aux problèmes éventuels et sensibiliser le public à la protection des données, si nécessaire conjointement avec les autorités nationales de contrôle.

[21] 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).

3. Aux fins prévues au paragraphe 2, le Contrôleur européen de la protection des données doit rencontrer les autorités de contrôle nationales au moins deux fois par an dans le cadre du comité européen de la protection des données. Le coût et l'organisation de ces réunions sont à la charge du comité européen de la protection des données. Le règlement intérieur est adopté lors de la première réunion. D'autres méthodes de travail sont mises au point d'un commun accord, en fonction des besoins.

4. Un rapport d'activités conjoint relatif au contrôle conjoint est transmis tous les deux ans au Parlement européen, au Conseil et à la Commission par le comité européen de la protection des données.

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 autre 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 la personne concernée 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 ladite réclamation, la réclamation est réputée avoir été rejetée.

Article 64
Droit à un recours juridictionnel effectif

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

Article 65
Droit à réparation

Toute personne ayant subi un dommage matériel ou un préjudice moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant 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 infliger 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 n'obtempère pas à un ordre du Contrôleur européen de la protection des données émis en vertu de l'article 59, 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 l'étendue 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 conformément aux 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) lorsque des mesures prévues à l'article 59, ont été précédemment ordonnées contre l'institution ou l'organe de l'Union concerné(e) pour le même objet, le respect de ces mesures;

Les procédures conduisant à infliger ces amendes devraient être menées dans un délai raisonnable en fonction des circonstances propres à chaque cas, en tenant compte des actions et procédures applicables mentionnées 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, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 et 46 doit, conformément au paragraphe 1, faire l'objet d'amendes administratives pouvant aller jusqu'à 25 000 EUR par violation et 250 000 EUR par an.

3. Toute violation des dispositions concernant les éléments suivants par l'institution ou l'organe de l'Union doit, conformément au paragraphe 1, faire l'objet d'amendes administratives pouvant aller jusqu'à 50 000 EUR par violation et 500 000 EUR par an:

(a) les principes de base d'un traitement, y compris les conditions applicables au consentement définis aux 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 47 à 51.

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 la possibilité de faire connaître son point de vue au sujet des griefs que le Contrôleur 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 assurés 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 qu'il en aille 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 infligeant des amendes en vertu du présent article font partie des recettes du budget général de l'Union européenne.

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 et 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 dans le cadre de la protection des données à caractère personnel les concernant, pour qu'il introduise une réclamation auprès du Contrôleur européen de la protection des données en son nom, exerce en son nom les droits prévus à l'article 63 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, 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

Tout manquement aux obligations énoncées dans le présent règlement auxquelles un fonctionnaire ou un autre agent de l'Union européenne est tenu, commis intentionnellement ou par négligence, l'expose à une sanction disciplinaire ou à une autre sanction, conformément aux dispositions du statut des fonctionnaires de l'Union européenne ou au régime applicable aux autres agents de l'Union européenne.

CHAPITRE IX

ACTES D'EXÉCUTION

Article 70
Procédure de 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 X

DISPOSITIONS FINALES

Article 71
Abrogation du règlement (CE) n° 45/2001 et de la décision n° 1247/2002/CE.

Le règlement (CE) n° 45/2001[22] et la décision n° 1247/2002/CE[23] sont abrogés avec effet au 25 mai 2018. Les références faites au règlement et à la décision abrogés s'entendent comme faites au présent règlement.

[22] 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).

[23] Décision n° 1247/2002/CE 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).

Article 72
Mesures transitoires

1. Le présent règlement ne porte pas atteinte à la décision 2014/886/UE du Parlement européen et du Conseil[24] ni aux mandats actuels du Contrôleur européen de la protection des données et du contrôleur adjoint.

2. La fonction de contrôleur adjoint est considérée comme équivalente à celle de greffier de la Cour de justice de l'Union européenne 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 54, paragraphes 4, 5 et 7, et les articles 56 et 57 du présent règlement s'appliquent à l'actuel contrôleur adjoint jusqu'à la fin de son mandat, le 5 décembre 2019.

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 de son mandat du contrôleur adjoint, le 5 décembre 2019.

Article 73
Entrée en vigueur et application

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

2. Il est applicable à partir du 25 mai 2018.

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

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*

[24] 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).

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaine(s) politique(s) concerné(s) dans la structure ABM/ABB

1.3. Nature de la proposition/de l'initiative

1.4. Objectif(s)

1.5. Justification(s) de la proposition/de l'initiative

1.6. Durée et incidence financière

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système de gestion et de contrôle

2.3. Mesures de prévention des fraudes et irrégularités

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

3.2. Incidence estimée sur les dépenses

3.2.1. Synthèse de l'incidence estimée sur les dépenses

3.2.2. Incidence estimée sur les crédits opérationnels

3.2.3. Incidence estimée sur les crédits de nature administrative

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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.

1.2. Domaine(s) politique(s) concerné(s) dans la structure ABM/ABB[25]

Justice - Protection des données à caractère personnel

1.3. Nature de la proposition/de l'initiative

☐ La proposition/l'initiative porte sur une **action nouvelle**

☐ La proposition/l'initiative porte sur une **action nouvelle suite à un projet pilote/une action préparatoire**[26]

– La proposition/l'initiative est relative à **la prolongation d'une action existante**

☐ La proposition/l'initiative porte sur **une action réorientée vers une nouvelle action**

1.4. Objectif(s)

1.4.1. Objectif(s) stratégique(s) pluriannuel(s) de la Commission visé(s) par la proposition/l'initiative

L'entrée en vigueur du traité de Lisbonne, notamment l'introduction d'une nouvelle base juridique (article 16 du TFUE), donne la possibilité d'établir un cadre global de protection des données couvrant tous les domaines.

Le 27 avril 2016, l'Union a adopté le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (texte présentant de l'intérêt pour l'EEE), JO L 119 du 4.5.2016, p. 1.

[25] ABM: activity-based management (gestion par activité); ABB: activity-based budgeting (établissement du budget par activité).

[26] Tel(le) que visé(e) à l'article 54, paragraphe 2, point a) ou b), du règlement financier.

Le même jour, l'Union a adopté la 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).

La présente proposition vise à achever l'établissement d'un cadre global de protection des données dans l'Union en alignant les règles de protection des données applicables aux institutions et organes de l'Union sur les règles en la matière du règlement (UE) 2016/679. Pour des raisons d'homogénéité et de cohérence, les institutions et organes de l'Union devraient appliquer un ensemble de règles de protection des données similaire à celui du secteur public dans les États membres.

1.4.2. Objectif(s) spécifique(s) et activité(s) ABM/ABB concernée(s)

Objectif spécifique nº 1:

Garantir une application cohérente des règles relatives à la protection des données dans l'ensemble de l'Union

Objectif spécifique nº 2:

Rationaliser le modèle de gouvernance actuel de la protection des données au sein des institutions et organes de l'Union

Objectif spécifique nº 3:

Garantir une application et un respect renforcés des règles en matière de protection des données au sein des institutions et organes de l'Union

1.4.3. Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

En leur qualité de responsables du traitement, les institutions et organes de l'Union devraient tirer profit du passage des procédures administratives actuelles (approche ex ante) associées à la protection des données à un respect effectif et une application renforcée des règles matérielles de protection des données et des nouveaux principes et concepts de protection des données introduits par le règlement (UE) 2016/679 (approche ex post), qui seront applicables dans l'ensemble de l'Union.

Les personnes physiques dont les données font l'objet d'un traitement par les institutions et organes de l'UE bénéficieront d'un meilleur contrôle de leurs données à caractère personnel et pourront avoir confiance dans l'environnement numérique. Elles constateront en outre que la responsabilité des institutions et organes de l'Union sera renforcée.

Le Contrôleur européen de la protection des données pourra se concentrer davantage sur sa fonction de contrôle. La répartition de la tâche consistant à conseiller la Commission entre le comité européen de la protection des données institué par le règlement (UE) 2016/679 et le Contrôleur européen de la protection des données sera clarifiée et les doubles emplois seront évités.

1.4.4. Indicateurs de résultats et d'incidences

Préciser les indicateurs permettant de suivre la réalisation de la proposition/de l'initiative.

Les indicateurs comprennent les éléments suivants:

le nombre d'avis émis par le comité européen de la protection des données et le Contrôleur européen de la protection des données,

la ventilation des activités des délégués à la protection des données,

le recours aux analyses d'impact relatives à la protection des données,

le nombre de plaintes introduites par des personnes concernées,

les amendes infligées aux responsables du traitement de données en raison de violations de la protection des données qui leur sont imputables.

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme

Dans le règlement (UE) 2016/679 [article 2, paragraphe 3), article 98, considérant 17], les colégislateurs de l'Union ont demandé une adaptation du règlement (CE) n° 45/2001 aux principes et règles fixés dans le règlement (UE) 2016/679, afin de mettre en place un cadre de protection des données solide et cohérent dans l'Union et de permettre l'application des deux instruments en même temps, soit le 25 mai 2018.

1.5.2. Valeur ajoutée de l'intervention de l'UE

Les règles de protection des données applicables aux institutions et organes de l'Union ne peuvent être introduites que par un acte de l'UE.

1.5.3. Leçons tirées d'expériences similaires

La présente proposition s'appuie sur l'expérience acquise avec le règlement (CE) n° 45/2001 et sur l'examen de son application réalisé dans le cadre d'une étude d'évaluation (conduite par un contractant externe de septembre 2014 à juin 2015)[27].

1.5.4. Compatibilité et synergie éventuelle avec d'autres instruments appropriés

La présente proposition s'appuie sur le règlement (UE) 2016/679 et achève l'établissement d'un cadre de protection des données solide, cohérent et moderne dans l'UE qui soit neutre sur le plan technologique et résistant à l'épreuve du temps.

[27] JUST/2013/FRAC/FW/0157/A4 dans le cadre du contrat-cadre multiple JUST/2011/EVAL/01 (RS 2013/05) - Étude d'évaluation sur le règlement (CE) n° 45/2001, par Ernst et Young.

1.6. Durée et incidence financière

☐Proposition/initiative **à durée limitée**

– ☐ Proposition/initiative en vigueur à partir de [JJ/MM]AAAA jusqu'en [JJ/MM]AAAA

– ☐ Incidence financière de AAAA jusqu'en AAAA

- Proposition/initiative **à durée illimitée**
- Mise en œuvre avec une période de montée en puissance de [2017] jusqu'au 25 mai 2018, puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) de gestion prévu(s)[28]

- Gestion directe par la Commission

– ☐ dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives.

☐ **Gestion partagée** avec les États membres

☐ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

– ☐ à des pays tiers ou aux organismes qu'ils ont désignés;

– ☐ à des organisations internationales et à leurs agences (à préciser);

– ☐ à la BEI et au Fonds européen d'investissement;

– ☐ aux organismes visés aux articles 208 et 209 du règlement financier;

– ☐ à des organismes de droit public;

– ☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

– ☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

– ☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

[28] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_fr.html

– *Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

Remarques

La présente proposition est limitée aux institutions et organes de l'Union et concerne l'ensemble de ceux-ci.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

La présente proposition est limitée à l'application des règles de protection des données par les institutions et organes de l'Union. Le contrôle et l'application de ces règles étant une compétence du Contrôleur européen de la protection des données, c'est lui qui assure le suivi et le compte rendu. En vertu de l'article 60 de la présente proposition, le Contrôleur européen de la protection des données est tenu en particulier de présenter au Parlement européen, au Conseil et à la Commission un rapport annuel sur ses activités, qu'il doit en même temps rendre public.

2.2. Système de gestion et de contrôle

2.2.1. Risque(s) identifié(s)

De septembre 2014 à juin 2015, un contractant externe a réalisé une étude d'évaluation sur l'application du règlement (CE) n° 45/2001. Cette étude examine également l'impact de l'introduction des principes et concepts essentiels du règlement (UE) 2016/679 au sein des institutions et organes de l'Union.

Le nouveau modèle de protection des données mettra l'accent sur le respect effectif des règles de protection des données, ainsi que sur l'application et le contrôle effectifs de ces règles. Il nécessitera une évolution de la culture en matière de protection des données dans les institutions et organes de l'Union, qui devra passer d'une approche ex ante administrative à une approche ex post effective.

2.2.2. Informations concernant le système de contrôle interne mis en place

Méthodes de contrôle existantes appliquées par les institutions et organes de l'Union.

2.2.3. Estimation du coût et des avantages des contrôles et évaluation du niveau attendu de risque d'erreur

Méthodes de contrôle existantes appliquées par les institutions et organes de l'Union.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées.

Méthodes existantes de prévention des fraudes appliquées par les institutions et organes de l'Union.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

- Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Type de dépense	Participation			
	Numéro [Rubrique……...……]	CD/CND[29] .	de pays AELE[30]	de pays candidats[31]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
	[XX.YY.YY.YY]	CD/CND	OUI/NON	OUI/NON	OUI/NON	OUI/NON

- Nouvelles lignes budgétaires, dont la création est demandée

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Type de dépense	Participation			
	Numéro [Rubrique……...……]	CD/CND	de pays AELE	de pays candidats	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
	[XX.YY.YY.YY]		OUI/NON	OUI/NON	OUI/NON	OUI/NON

[29] CD = crédits dissociés / CND = crédits non dissociés.

[30] AELE: Association européenne de libre-échange.

[31] Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

3.2. Incidence estimée sur les dépenses

L'incidence de la présente proposition est limitée aux dépenses des institutions et organes de l'Union. L'évaluation des coûts liés à la présente proposition montre toutefois que cette dernière n'engendre pas de dépenses supplémentaires substantielles pour les institutions et organes de l'Union.

En ce qui concerne les responsables du traitement des données au sein des institutions et organes de l'Union, l'étude d'évaluation relative à l'application du règlement (CE) n° 45/2001 montre que leurs activités de protection des données correspondent à environ 70 équivalents temps plein (ETP), soit environ 9 300 000 EUR par an. Ils consacrent actuellement environ 20 % de leurs activités de protection des données à des notifications de traitement de données. Le présent règlement supprime cette activité, ce qui correspond à une économie annuelle de 1 922 000 EUR pour les responsables du traitement des données au sein des institutions et organes de l'Union. Cette économie devrait être contrebalancée par une implication accrue des responsables du traitement dans la mise en œuvre des nouveaux principes et concepts introduits par le présent règlement.

Plus précisément, l'examen réalisé dans le cadre de l'étude d'évaluation a souligné que:

a) l'introduction du principe de minimisation des données aurait peu ou pas d'incidences sur les institutions et organes de l'Union;

b) l'introduction du principe de transparence n'aurait pas d'incidence significative sur les institutions et organes de l'Union;

c) le renforcement des obligations d'information alourdirait la charge de travail des responsables du traitement des données et des délégués à la protection des données;

d) l'introduction du droit à l'oubli n'aurait pas d'incidence significative sur les institutions et organes de l'Union;

e) l'introduction du principe de portabilité des données aurait peu ou pas d'incidences sur les institutions et organes de l'Union;

f) l'introduction d'analyses d'impact relatives à la protection des données aurait une incidence moyennement importante sur la charge de travail des responsables du traitement et des délégués à la protection des données, étant donné que certaines institutions et organes de l'Union procèdent déjà à de telles analyses et que les cas dans lesquels celles-ci seront nécessaires sont limités;

g) l'introduction de notifications de violations de données à caractère personnel alourdirait la charge de travail des responsables du traitement, mais de telles violations sont rares;

g) la protection des données dès la conception et la protection des données par défaut sont déjà en vigueur dans plusieurs institutions et organes de l'Union.

En outre, l'analyse d'impact réalisée avant l'adoption de la proposition de réforme de la protection des données a conclu que l'introduction du principe de protection des données dès la conception n'engendrerait pas de charge administrative pour les pouvoirs publics ni pour les responsables du traitement des données[32].

En ce qui concerne les délégués à la protection des données, l'étude d'évaluation a estimé le coût du réseau actuel des délégués à la protection des données et des coordinateurs de la protection des données (les «DPD» et les «CPD») des institutions et organes de l'Union à 82,9 ETP ou 10 900 000 EUR par an. Ils consacrent 26 % du temps alloué à la protection des données à des activités qui seraient supprimées par le présent règlement, à savoir la rédaction de notifications (à la place des responsables du traitement), l'évaluation des notifications reçues, la consignation de leurs activités dans le registre et la réalisation de contrôles préalables. Ces suppressions d'activités engendrent une économie supplémentaire de 2 834 000 EUR par an pour les institutions et organes de l'Union. En outre, le présent règlement offre un potentiel d'économies supplémentaires en permettant aux institutions et organes de l'Union d'externaliser des activités des DPD plutôt que de recourir à leur propre personnel.

Les économies associées aux activités des DPD seront contrebalancées par l'association de ces derniers aux obligations d'information renforcées, aux analyses d'impact relatives à la protection des données (dans des circonstances limitées lorsque celles-ci seront nécessaires) et à la consultation préalable du Contrôleur européen de la protection des données (dont le champ d'action sera nettement plus limité que dans le cadre de l'obligation actuelle de contrôle préalable).

En ce qui concerne le Contrôleur européen de la protection des données, son budget annuel est assez stable depuis 2011 et tourne autour de 8 000 000 EUR. Actuellement, son unité «Supervision et mise en application» et son unité «Politique et consultation» sont dotées d'effectifs comparables, stables depuis 2008. L'accent renforcé mis par le présent règlement sur la fonction de contrôle du Contrôleur européen de la protection des données sera compensé par un ciblage plus important de sa fonction de conseil et par une élimination des doubles emplois avec le comité européen de la protection des données. Le Contrôleur européen de la protection des données peut donc procéder à une réaffectation interne de son personnel.

[32] Document de travail des services de la Commission, Analyse d'impact, SEC(2012) 72 final, p. 110.

La présente proposition prévoit la possibilité que le Contrôleur européen de la protection des données inflige des amendes administratives aux institutions et organes de l'Union. Chaque institution ou organe de l'Union peut se voir infliger une amende pouvant atteindre un montant maximum de 250 000 EUR par an (25 000 EUR par infraction) ou de 500 000 EUR par an (50 000 EUR par infraction) pour les infractions les plus graves prévues par le présent règlement. Ces amendes devraient être infligées uniquement dans les cas les plus graves et à la suite du non-respect par l'institution ou l'organe concerné de l'Union d'autres mesures correctrices adoptées par le Contrôleur européen de la protection des données en vertu des pouvoirs qui lui sont conférés. L'incidence financière de ces amendes devrait donc être limitée.

3.2.1. Synthèse de l'incidence estimée sur les dépenses

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	Numéro	[Rubrique……...……]

DG: <…….>			Année **N**[33]	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			**TOTAL**
• Crédits opérationnels										
Numéro de ligne budgétaire	Engagements	(1)								
	Paiements	(2)								
Numéro de ligne budgétaire	Engagements	(1a)								
	Paiements	(2a)								
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[34]										
Numéro de ligne budgétaire		(3)								

33 L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative.

34 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

TOTAL des crédits pour la DG <…….>	Engagements	=1+1a +3								
	Paiements	=2+2a +3.								

• TOTAL des crédits opérationnels	Engagements	(4)								
	Paiements	(5)								
• TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		(6)								
TOTAL des crédits pour la RUBRIQUE <….> du cadre financier pluriannuel	Engagements	=4+ 6								
	Paiements	=5+ 6								

Si plusieurs rubriques sont concernées par la proposition/l'initiative:

• TOTAL des crédits opérationnels	Engagements	(4)								
	Paiements	(5)								
• TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		(6)								
TOTAL des crédits pour les RUBRIQUES 1 à 4 du cadre financier pluriannuel (Montant de référence)	Engagements	=4+ 6								
	Paiements	=5+ 6								

Rubrique du cadre financier pluriannuel	**5.**	«Dépenses administratives»

En Mio EUR (à la 3e décimale)

		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			**TOTAL**
DG: <…….>									
• Ressources humaines									
•Autres dépenses administratives									
TOTAL DG <….>	Crédits								

TOTAL des crédits pour la RUBRIQUE 5 du cadre financier pluriannuel	(Total engagements = Total paiements)								

En Mio EUR (à la 3e décimale)

		Année **N**[35]	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 5 du cadre financier pluriannuel	Engagements								
	Paiements								

[35] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative.

3.2.2. Incidence estimée sur les crédits opérationnels

- La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

☐ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations ⇩			Année **N**		Année **N+1**		Année **N+2**		Année **N+3**		Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)						**TOTAL**	
	RÉALISATIONS (outputs)																	
	Type[36]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE n° 1[37]...																		
- Réalisation																		
- Réalisation																		
- Réalisation																		
Sous-total objectif spécifique n° 1																		
OBJECTIF SPÉCIFIQUE n° 2…																		
- Réalisation																		
Sous-total objectif spécifique n° 2																		
COÛT TOTAL																		

[36] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[37] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

3.2.3. Incidence estimée sur les crédits de nature administrative

3.2.3.1. Synthèse

- La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

☐ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année N[38]	Année N+1	Année N+2	Année N+3	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			**TOTAL**
RUBRIQUE 5 du cadre financier pluriannuel								
Ressources humaines								
Autres dépenses administratives								
Sous-total RUBRIQUE 5 du cadre financier pluriannuel								
Hors RUBRIQUE 5[39] du cadre financier pluriannuel								
Ressources humaines								
Autres dépenses de nature administrative								
Sous-total hors RUBRIQUE 5 du cadre financier pluriannuel								
TOTAL								

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

38 L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative.

39 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

3.2.3.2. Besoins estimés en ressources humaines

- La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

☐ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en équivalents temps plein

	Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)		
• Emplois du tableau des effectifs (fonctionnaires et agents temporaires)							
XX 01 01 01 (au siège et dans les bureaux de représentation de la Commission)							
XX 01 01 02 (en délégation)							
XX 01 05 01 (recherche indirecte)							
10 01 05 01 (recherche directe)							
•Personnel externe (en équivalents temps plein: ETP)[40]							
XX 01 02 01 (AC, END, INT de l'enveloppe globale)							
XX 01 02 02 (AC, AL, END, INT et JED dans les délégations)							
XX 01 04 **yy** [41] - au siège							
XX 01 04 **yy** [41] - en délégation							
XX 01 05 02 (AC, END, INT sur recherche indirecte)							
10 01 05 02 (AC, END, INT sur recherche directe)							
Autres lignes budgétaires (à préciser)							
TOTAL							

XX est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

[40] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JED = jeune expert en délégation.

[41] Sous-plafonds de personnel externe financés sur crédits opérationnels (anciennes lignes «BA»).

Fonctionnaires et agents temporaires	
Personnel externe	

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

- La proposition/l'initiative est compatible avec le cadre financier pluriannuel actuel.

☐ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

Expliquez la reprogrammation requise, en précisant les lignes budgétaires concernées et les montants correspondants.

☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants.

3.2.5. Participation de tiers au financement

- La proposition/l'initiative ne prévoit pas de cofinancement par des tierces parties.

La proposition/l'initiative prévoit un cofinancement estimé ci-après:

Crédits en Mio EUR (à la 3e décimale)

	Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			Total
Préciser l'organisme de cofinancement								
TOTAL crédits cofinancés								

3.3. Incidence estimée sur les recettes

- La proposition/l'initiative est sans incidence financière sur les recettes.

☐ La proposition/l'initiative a une incidence financière décrite ci-après:

– ☐ sur les ressources propres

– ☐ sur les recettes diverses

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[42]						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)		
Article …….								

Pour les recettes diverses qui seront «affectées», préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

Préciser la méthode de calcul de l'incidence sur les recettes.

[42] En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 25 % de frais de perception.