N° 7373

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

[…] concernant la limitation de la portée de certains droits et obligations dans le cadre du règlement général sur la protection des données et portant :

1. **exécution, en matière de surveillance du secteur financier et des assurances, du 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) ;**
2. **modification de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et**
3. **modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances**

* * *

(Dépôt: le 22.10.2018)

SOMMAIRE:

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre des Finances et après délibération du Gouvernement en conseil ;

Arrêtons:

Article unique.– Notre Ministre des Finances est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi du […] concernant la limitation de la portée de certains droits et obligations dans le cadre du règlement général sur la protection des données et portant :

1. exécution, en matière de surveillance du secteur financier et des assurances, du 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) ;
2. modification de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et
3. modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances.

Palais de Luxembourg, le 15 octobre 2018

Le Ministre des Finances,
Pierre GRAMEGNA

HENRI

*

EXPOSE DES MOTIFS

Le projet de loi a pour but d'introduire dans la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier et dans la loi modifiée du 7 décembre 2015 sur le secteur des assurances des limitations facultatives visant à restreindre la pleine application de certaines dispositions du 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) (ci-après, le « Règlement (UE) 2016/679 »).

En effet, les articles 6 et 23 du Règlement (UE) 2016/679 prévoient que le droit d'un Etat membre peut, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus notamment aux articles 12 à 22 et 34 du Règlement (UE) 2016/679. De telles limitations facultatives sont permises par ledit règlement si elles respectent l'essence des libertés et droits fondamentaux et constituent une mesure nécessaire et proportionnée dans une société démocratique pour garantir l'un des objectifs prévus limitativement à l'article 23, paragraphe 1er, du Règlement (UE) 2016/679, et à la condition que cette mesure législative prévoie des dispositions spécifiques relatives, au moins, aux éléments visés à l'article 23, paragraphe 2, dudit règlement. Des considérations d'intérêt général sont donc susceptibles, dans des situations bien limitées, de supplanter les considérations d'intérêt privé dont relève la protection des données personnelles. Les dérogations prévues dans le présent projet de loi qui sont prises en vertu de l'article 23 du Règlement (UE) 2016/679 ne peuvent être prévues et mises en œuvre sans prévoir en contrepartie des garanties appropriées, afin de ne pas mettre en cause l'essence des droits fondamentaux des personnes concernées.

Le projet de loi vise ainsi à compléter les limitations générales prévues dans le Règlement (UE) 2016/679 par des limitations spécifiques dans le domaine des compétences de la Commission de surveillance du secteur financier (ci-après, la « CSSF ») et du Commissariat aux assurances (ci-après, le « CAA »), en vue d'assurer dans tous les cas un exercice efficace des missions de la CSSF et du CAA dans les cadres luxembourgeois, européen et international, et pour garantir en même temps un haut degré de protection des données à caractère personnel. Les limitations prévues par le présent projet de loi ne pourront jamais être appliquées en tant que restrictions générales aux droits de la personne concernée ou aux obligations de la CSSF et du CAA découlant du Règlement (UE) 2016/679, mais

uniquement dans des cas bien délimités et lorsqu'il est indispensable de le faire. La CSSF et le CAA devront en effet respecter en principe les droits fondamentaux en matière de protection des données des personnes concernées. Les limitations prévues dans le présent projet de loi ne sont mises en œuvre que si leurs conditions légales sont respectées et si ces limitations respectent le principe de proportionnalité. Le projet de loi exige que, dans le cadre de cette appréciation, la CSSF et le CAA tiennent compte de toutes les circonstances factuelles et juridiques du cas qui se présente à eux. Parallèlement, le texte du projet de loi prévoit des dispositions protectrices (garanties) qui ont vocation à compenser une limitation et donc à maintenir un haut degré de protection dans le chef des personnes concernées.

*

TEXTE DU PROJET DE LOI

Art. I^er^. 1° A l'article 3 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier, il est réintroduite entre les lettres b) et d) une nouvelle lettre c), libellée comme suit :

« c) est autorisée à effectuer le traitement de données à caractère personnel dans le cadre de l'application des compétences légales de la CSSF, et en vue des finalités visées aux articles 2 à 2-3 et dans les lois sectorielles qui y sont référencées et qui déterminent les missions, compétences et pouvoirs de la CSSF ; ».

2° A la suite de l'article 16 de la même loi, sont insérés les articles 16-1 à 16-9, libellés comme suit :

« **Art. 16-1.** (1) La CSSF est autorisée à collecter et à traiter des données à caractère personnel qui sont nécessaires à l'exercice de ses missions. Ces données à caractère personnel comprennent les données personnelles qui sont indiquées sur les documents officiels ou autres déclarations que les personnes concernées fournissent elles-mêmes ou qui sont transmises par des intermédiaires agissant pour ces personnes, ou qui sont collectées auprès de ces personnes ou auprès de tiers. Les données à caractère personnel collectées et traitées peuvent également concerner des données économiques ou financières des personnes concernées.

(2) La collecte et le traitement des données à caractère personnel visés au paragraphe 1^er^ sont sans préjudice de l'obligation au secret professionnel prévue à l'article 16.

Art. 16-2. Sans préjudice de l'article 6, paragraphe 4, du 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), désigné ci-après « Règlement (UE) 2016/679 », le traitement des données à caractère personnel par la CSSF à une fin autre que celle pour laquelle les données ont été collectées dans le cadre de ses compétences légales est autorisé si :

a) le traitement est effectué dans le cadre d'une procédure ayant pour objet d'imposer une sanction administrative, une mesure de police administrative ou une mesure prudentielle, ou dans le cadre d'actes préparatoires, dans un processus d'audit, de contrôle ou dans le contexte d'une procédure juridictionnelle ;

b) le traitement sert à assurer l'exercice des missions de la CSSF ainsi que le respect des obligations qui en découlent dans le chef de la CSSF, y compris en matière de coopération avec d'autres institutions, autorités, organes ou organismes nationaux, étrangers, européens et internationaux, telle que prévue dans les lois sectorielles régissant lesdites missions ;

c) le traitement est nécessaire pour la poursuite d'une procédure administrative au niveau européen à laquelle la CSSF est partie ;

d) le traitement de données personnelles non pseudonymisées est nécessaire au développement, au contrôle ou à la modification des procédures internes de fonctionnement de la CSSF ; ou

e) le traitement de données personnelles non pseudonymisées est nécessaire pour assurer l'audit de la CSSF, de la direction et des procédures disciplinaires internes de la CSSF.

Art. 16-3. L'obligation de la CSSF de fournir tout ou partie des informations visées à l'article 13, paragraphes 1er, 2 et 3, du Règlement (UE) 2016/679 à la personne concernée lorsque des données personnelles sont collectées auprès d'elle, peut être limitée ou différée par la CSSF dans les cas suivants :

a) lorsque la transmission de ces informations compromet, ou risque de compromettre, l'exercice des missions et compétences prévues aux articles 2 à 2-3 et des pouvoirs légaux de la CSSF, pour autant que l'intérêt poursuivi par la CSSF de ne pas informer la personne concernée prime sur l'intérêt privé de celle-ci.

   L'exercice des missions et compétences de la CSSF peut être compromis lorsque la personne concernée fait l'objet d'une procédure administrative ou d'une procédure ayant pour objet d'imposer une sanction administrative, une mesure de police administrative ou une mesure prudentielle, ou lorsque cette personne fait l'objet d'une enquête, ou d'actes préparatoires à ces procédures ou enquêtes, lorsque ces procédures ou enquêtes sont effectuées par la CSSF dans le cadre de l'exécution de ses missions légales, et lorsque l'obligation de la CSSF de respecter pleinement ou immédiatement les droits de la personne concernée ou le plein ou immédiat exercice des droits de la personne concernée porterait atteinte aux besoins ou objectifs de ces procédures ou enquêtes, ou aux actes préparatoires.

   Il en est notamment ainsi, si le plein ou immédiat exercice des droits de la personne concernée ou la pleine ou immédiate exécution des obligations de la CSSF est susceptible de mettre la personne concernée ou des tiers dans une situation permettant d'occulter des faits ou des informations pertinentes dans le cadre desdites procédures ou enquêtes de la CSSF, ou encore d'en tirer un avantage illégitime au détriment de l'exercice des pouvoirs et missions de la CSSF. La CSSF ne peut limiter ou différer son obligation de fournir tout ou partie des informations visées au paragraphe 1er que pendant la durée nécessaire à atteindre la finalité qui justifie la limitation des droits ;

b) si le plein ou immédiat exercice des droits de la personne concernée ou la pleine ou immédiate exécution des obligations de la CSSF menace la stabilité du système bancaire et financier ou des marchés, le maintien de l'ordre public ou la sécurité publique, pour autant que la protection de ces intérêts publics légitimes prévaut sur les intérêts privés de la personne concernée ;

c) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF entrave la défense des intérêts légitimes de la CSSF liés à l'exercice de ses missions légales dans le cadre de procédures juridictionnelles ;

d) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF entrave la poursuite par la CSSF d'une procédure administrative dans laquelle elle est partie, en ce comprise, mais sans s'y limiter, une procédure administrative en non-application ou en violation du droit de l'Union européenne telle que prévue dans le règlement (UE) n°1093/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité bancaire européenne), le règlement (UE) n°1094/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), et le règlement (UE) n°1095/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des marchés financiers) ;

e) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF entrave la communication confidentielle et licite de données en provenance d'autorités ou d'organismes nationaux, étrangers, européens ou internationaux qui transmettent ces données dans l'exercice de leurs compétences respectives, ou qui leur sont transmises par la CSSF dans le cadre de l'exercice de ses compétences légales ;

f) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF porte atteinte à des intérêts légitimes protégés de tiers.

Art. 16-4. L'obligation de la CSSF de fournir tout ou partie des informations visées à l'article 14, paragraphes 1er, 2 et 4, du Règlement (UE) 2016/679 à la personne concernée lorsque des données personnelles sont collectées auprès d'un tiers, peut être limitée ou différée dans les cas visés à l'article 16-3, lettres a) à f), pour autant que l'intérêt public poursuivi par la CSSF de ne pas fournir à la personne concernée ces informations prime sur l'intérêt privé de la personne concernée.

Art. 16-5. Dans les cas visés à l'article 16-3, lettres a) à f), et pour autant que l'intérêt public poursuivi par la CSSF prime sur l'intérêt privé de la personne concernée, la CSSF peut :

a) limiter ou différer la confirmation à la personne concernée que des données à caractère personnel sont traitées, telle que prévue à l'article 15, paragraphe 1er, du Règlement (UE) 2016/679 ;

b) limiter ou différer l'accès, tel que prévu à l'article 15, paragraphe 1er, du Règlement (UE) 2016/679, auxdites données lorsqu'elle procède à un traitement de données à caractère personnel ;

c) limiter ou différer la transmission de tout ou partie des informations visées à l'article 15, paragraphes 1er et 2, du Règlement (UE) 2016/679.

Art. 16-6. La CSSF peut limiter ou différer l'exercice par la personne concernée de son droit à la limitation du traitement de ses données personnelles, tel que prévu à l'article 18 du Règlement (UE) 2016/679, dans les cas visés à l'article 16-3, lettres a) à f), pour autant que l'intérêt public poursuivi par la CSSF de procéder au traitement prime sur l'intérêt privé de la personne concernée.

Art. 16-7. La CSSF peut limiter ou différer le droit de la personne concernée de s'opposer au traitement de ses données à caractère personnel, tel que prévu à l'article 21, paragraphe 1er, du Règlement (UE) 2016/679, dans les cas visés à l'article 16-3, lettres a) à f), pour autant que l'intérêt public poursuivi par la CSSF de procéder au traitement prime sur l'intérêt privé de la personne concernée.

Art. 16-8. (1) Lorsque la CSSF diffère ou limite, en tout ou en partie, les droits de la personne concernée ou ses propres obligations découlant du Règlement (UE) 2016/679 en application d'une disposition prévue aux articles 16-3 à 16-7, la CSSF lève la limitation à partir du moment où la cause qui la justifie cesse d'exister ou cesse de produire ses effets.

(2) La CSSF informe la personne concernée, par écrit et dans le mois de la survenance de la cause qui justifie la limitation ou le retard, de l'existence de la limitation ou du retard concernant l'exercice par la personne concernée de ses droits ou de ses propres obligations, ainsi que des motifs de la limitation ou retard, à moins que ces informations ne risquent de nuire à la finalité du traitement, de la limitation ou du retard, notamment lorsque ces informations violent le secret professionnel auquel est tenue la CSSF en application de l'article 16, ou lorsque ces informations empêchent la CSSF de poursuivre une procédure administrative ou juridictionnelle à laquelle la CSSF est partie.

(3) La CSSF consigne par écrit les motifs de fait et de droit sur lesquels se fonde sa décision de limiter ou de différer les droits de la personne concernée ou ses propres obligations découlant du Règlement (UE) 2016/679 prise en application d'une disposition prévue aux articles 16-3 à 16-7. Lorsqu'un droit d'une personne concernée ou l'une des obligations incombant à la CSSF est limité ou différé, la CSSF indique la date à partir de laquelle cette limitation deviendra caduque ou, à défaut de date précise, les circonstances permettant d'y mettre fin.

Ces informations sont mises à disposition de la Commission nationale pour la protection des données (ci-après, la « CNPD »), sans préjudice de l'obligation au secret professionnel visée à l'article 16.

(4) La CSSF informe les personnes concernées que leurs données à caractère personnel ont fait l'objet d'un traitement si une procédure administrative ou une enquête a été menée à leur encontre ou si ces personnes ont figuré comme tiers dans une procédure administrative ou une enquête, y compris dans les actes préparatoires, qui a été classée sans qu'une décision n'ait été prise par la CSSF, à moins que ces informations ne violent le secret professionnel visé à l'article 16. L'information leur est fournie sur un support adéquat au plus tard dans les deux mois suivant le classement de la procédure ou de l'enquête.

(5) En cas de limitation des droits de la personne concernée ou de ses propres obligations, la CSSF informe la personne concernée de la possibilité d'introduire une réclamation auprès de la CNPD, conformément à l'article 77 du Règlement (UE) 2016/679, à moins que ces informations ne risquent de nuire à la finalité du ou des traitements et de la limitation, notamment lorsque ces informations violent le secret professionnel auquel est tenue la CSSF en application de l'article 16, ou lorsque ces informations empêchent la CSSF de poursuivre une procédure administrative ou juridictionnelle à laquelle la CSSF est partie.

(6) Sans préjudice du droit de réclamation auprès de la CNPD, la CSSF informe la personne concernée de la possibilité de former un recours juridictionnel, à moins que cette information par la CSSF ne risque de nuire à la finalité du ou des traitements et de la limitation, que cette information viole le secret professionnel auquel est tenue la CSSF en application de l'article 16 ou que cette information empêche la CSSF de poursuivre une procédure administrative ou juridictionnelle à laquelle la CSSF est partie.

(7) La CSSF procède à une vérification régulière de ses systèmes informatiques et procédures internes afin de garantir la conformité du traitement des données à caractère personnel et des limitations aux droits de la personne concernée avec les dispositions du Règlement (UE) 2016/679.

(8) Les données à caractère personnel traitées conformément à la présente loi sont conservées aussi longtemps que nécessaire à l'exercice par la CSSF de ses compétences légales.

Art. 16-9. (1) En cas de limitation des droits de la personne concernée en vertu des articles 16-3 à 16-7, les droits limités ou différés de la personne concernée peuvent être exercés par la CNPD, sans préjudice du secret professionnel de la CSSF prévu à l'article 16.

(2) La CSSF informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la CNPD en application du paragraphe 1er, sauf si cette information nuit à la finalité du ou des traitements et de la limitation ou lorsque cette information viole le secret professionnel de la CSSF prévu à l'article 16 ou empêche la CSSF d'agir ou de se défendre dans une procédure administrative ou juridictionnelle.

(3) Lorsque le droit visé au paragraphe 1er est exercé, la CNPD peut communiquer à la personne concernée le résultat de ses investigations, à moins que cette information ne risque de nuire à la finalité du ou des traitements et de la limitation, que cette information viole le secret professionnel auquel est tenue la CSSF en application de l'article 16 ou que cette information empêche la CSSF de poursuivre une procédure administrative ou juridictionnelle à laquelle la CSSF est partie. Le cas échéant, la CNPD informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. Elle informe également la personne concernée de son droit de former un recours juridictionnel. »

Art. II. 1° A l'article 5 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, un nouvel alinéa 4 est inséré et libellé comme suit :

« Le CAA est autorisé, en vue des missions visées aux articles 2 et 3 et dans le cadre des pouvoirs énoncés à l'article 4, à effectuer un traitement de données à caractère personnel. »

2° A la suite de l'article 13 de la même loi, sont insérés de nouveaux articles 13-1 à 13-9, libellés comme suit :

« **Art. 13-1 –** ***Caractéristiques des données à caractère personnel et licéité de leur traitement***

(1) Le CAA est autorisé à collecter et à traiter des données à caractère personnel qui sont nécessaires à l'exercice de ses missions. Ces données à caractère personnel comprennent les données personnelles qui sont indiquées sur les documents officiels ou autres déclarations que les personnes concernées fournissent elles-mêmes ou qui sont transmises par des intermédiaires agissant pour ces personnes, ou qui sont collectées auprès de ces personnes ou auprès de tiers. Les données à caractère personnel collectées et traitées peuvent également concerner des données économiques ou financières des personnes concernées.

(2) La collecte et le traitement des données à caractère personnel visés au paragraphe 1er sont sans préjudice de l'obligation au secret professionnel prévue à l'article 7.

Art. 13-2 – ***Conditions de changement de la finalité du traitement des données à caractère personnel***

Sans préjudice de l'article 6, paragraphe 4, du Règlement (UE) 2016/679, le traitement des données à caractère personnel par le CAA à une fin autre que celle pour laquelle les données ont été collectées dans le cadre de ses compétences légales est autorisé si :

a) le traitement est effectué dans le cadre d'une procédure ayant pour objet d'imposer une sanction administrative, une mesure de police administrative ou une mesure prudentielle, ou dans le cadre

d'actes préparatoires, dans un processus d'audit, de contrôle ou dans le contexte d'une procédure juridictionnelle ;

b) le traitement sert à assurer l'exercice des missions du CAA ainsi que le respect des obligations qui en découlent dans le chef du CAA, y compris en matière de coopération avec d'autres institutions, autorités, organes ou organismes nationaux, étrangers, européens ou internationaux, telle que prévue dans les lois sectorielles régissant lesdites missions ;

c) le traitement est nécessaire pour la poursuite d'une procédure administrative au niveau européen à laquelle le CAA est partie ;

d) le traitement de données personnelles non pseudonymisées est nécessaire au développement, au contrôle ou à la modification des procédures internes de fonctionnement du CAA ;

e) le traitement de données non pseudonymisées est nécessaire pour assurer l'audit du CAA, de la direction et des procédures disciplinaires internes du CAA.

Art. 13-3 – ***Cas de limitation des droits et obligations prévus à l'article 13 du Règlement (UE) 2016/679***

L'obligation du CAA de fournir tout ou partie des informations visées à l'article 13, paragraphes 1er, 2 et 3, du Règlement (UE) 2016/679 à la personne concernée lorsque des données personnelles sont collectées auprès de lui, peut être limitée ou différée par le CAA dans les cas suivants :

a) lorsque la transmission de ces informations compromet, ou risque de compromettre, l'exercice des missions et compétences prévues aux articles 2 et 3 et des pouvoirs légaux du CAA prévus à l'article 4, pour autant que l'intérêt poursuivi par le CAA de ne pas informer la personne concernée prime sur l'intérêt privé de celle-ci.

L'exercice des missions et compétences du CAA peut être compromis lorsque la personne concernée fait l'objet d'une procédure administrative ou d'une procédure ayant pour objet d'imposer une sanction administrative, une mesure de police administrative ou une mesure prudentielle, ou lorsque cette personne fait l'objet d'une enquête, ou d'actes préparatoires à ces procédures ou enquêtes, lorsque ces procédures ou enquêtes sont effectuées par le CAA dans le cadre de l'exécution de ses missions légales, et lorsque l'obligation du CAA de respecter pleinement ou immédiatement les droits de la personne concernée ou le plein ou immédiat exercice des droits de la personne concernée porterait atteinte aux besoins ou objectifs de ces procédures ou enquêtes, ou aux actes préparatoires.

Il en est notamment ainsi, si le plein ou immédiat exercice des droits de la personne concernée ou la pleine ou immédiate exécution des obligations du CAA est susceptible de mettre la personne concernée ou des tiers dans une situation permettant d'occulter des faits ou des informations pertinentes dans le cadre desdites procédures ou enquêtes du CAA, ou encore d'en tirer un avantage illégitime au détriment de l'exercice des pouvoirs et missions de du CAA. Le CAA ne peut limiter ou différer son obligation de fournir tout ou partie des informations visées au paragraphe 1e que pendant la durée nécessaire à atteindre la finalité qui justifie la limitation des droits ;

b) si le plein ou immédiat exercice des droits de la personne concernée ou la pleine ou immédiate exécution des obligations du CAA menace la stabilité financière ou des marchés, le maintien de l'ordre public ou la sécurité publique, pour autant que la protection de ces intérêts publics légitimes prévaut sur les intérêts privés de la personne concernée ;

c) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations du CAA entrave la défense des intérêts légitimes du CAA liés à l'exercice de ses missions légales dans le cadre de procédures juridictionnelles ;

d) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations du CAA entrave la poursuite par le CAA d'une procédure administrative dans laquelle il est partie, en ce comprise, mais sans s'y limiter, une procédure administrative en non-application ou en violation du droit de l'Union européenne telle que prévue dans le règlement (UE) n°1093/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité bancaire européenne), le règlement (UE) n°1094/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), et le règlement (UE) n°1095/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des marchés financiers) ;

e) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations du CAA entrave la communication confidentielle et licite de données en provenance d'autorités ou d'organismes nationaux, étrangers, européens ou internationaux qui transmettent ces données dans l'exercice de leurs compétences respectives, ou qui leur sont transmises par le CAA dans le cadre de l'exercice de ses compétences légales ;

f) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations du CAA porte atteinte à des intérêts légitimes protégés de tiers.

Art. 13-4 – ***Cas de limitation des droits et obligations prévus à l'article 14 du Règlement (UE) 2016/679***

L'obligation du CAA de fournir tout ou partie des informations visées à l'article 14, paragraphes 1er, 2 et 4, du Règlement (UE) 2016/679 à la personne concernée lorsque des données personnelles sont collectées auprès d'un tiers, peut être limitée ou différée dans les cas visés à l'article 13-3, lettres a) à f), pour autant que l'intérêt public poursuivi par le CAA de ne pas fournir à la personne concernée ces informations prime sur l'intérêt privé de la personne concernée.

Art. 13-5 – ***Cas de limitation des droits et obligations prévus à l'article 15 du Règlement (UE) 2016/679***

Dans les cas visés à l'article 13-3, lettres a) à f), et pour autant que l'intérêt public poursuivi par le CAA prime sur l'intérêt privé de la personne concernée, le CAA peut :

a) limiter ou différer la confirmation à la personne concernée que des données à caractère personnel sont traitées, telle que prévue à l'article 15, paragraphe 1er, du Règlement (UE) 2016/679 ;

b) limiter ou différer l'accès auxdites données lorsqu'il procède à un traitement de données à caractère personnel ;

c) limiter ou différer la transmission de tout ou partie des informations visées à l'article 15, paragraphes 1er et 2, du Règlement (UE) 2016/679.

Art. 13-6 – ***Cas de limitation des droits et obligations prévus à l'article 18 du Règlement (UE) 2016/679***

Le CAA peut limiter ou différer l'exercice par la personne concernée de son droit à la limitation du traitement de ses données personnelles, tel que prévu à l'article 18 du Règlement (UE) 2016/679, dans les cas visés à l'article 13-3, lettres a) à f), pour autant que l'intérêt public poursuivi par le CAA de procéder au traitement prime sur l'intérêt privé de la personne concernée.

Art. 13-7 – ***Cas de limitation des droits et obligations prévus à l'article 21 du Règlement (UE) 2016/679***

Le CAA peut limiter ou différer le droit de la personne concernée de s'opposer au traitement de ses données à caractère personnel, tel que prévu à l'article 21, paragraphe 1er, du Règlement (UE) 2016/679, dans les cas visés à l'article 13-3, lettres a) à f), pour autant que l'intérêt public poursuivi par le CAA de procéder au traitement prime sur l'intérêt privé de la personne concernée.

Art. 13-8 – ***Obligations du CAA en cas de limitation des droits et obligations en matière de protection des données confidentielles***

(1) Lorsque le CAA diffère ou limite, en tout ou en partie, les droits de la personne concernée ou ses propres obligations découlant du Règlement (UE) 2016/679 en application d'une disposition prévue aux articles 13-3 à 13-7, le CAA lève la limitation à partir du moment où la cause qui la justifie cesse d'exister ou cesse de produire ses effets.

(2) Le CAA informe la personne concernée, par écrit et dans le mois de la survenance de la cause qui justifie la limitation ou le retard, de l'existence de la limitation ou du retard concernant l'exercice par la personne concernée de ses droits ou de ses propres obligations, ainsi que des motifs de la limitation ou retard, à moins que ces informations ne risquent de nuire à la finalité du traitement, de la limitation ou du retard, notamment lorsque ces informations violent le secret professionnel auquel est tenu le CAA en application de l'article 7, ou lorsque ces informations empêchent le CAA de poursuivre une procédure administrative ou juridictionnelle à laquelle le CAA est partie.

(3) Le CAA consigne par écrit les motifs de fait et de droit sur lesquels se fonde sa décision de limiter ou de différer les droits de la personne concernée ou ses propres obligations découlant du

Règlement (UE) 2016/679 prise en application d'une disposition prévue aux articles 13-3 à 13-7. Lorsqu'un droit d'une personne concernée ou l'une des obligations incombant au CAA est limité ou différé, le CAA indique la date à partir de laquelle cette limitation deviendra caduque ou, à défaut de date précise, les circonstances permettant d'y mettre fin.

Ces informations sont mises à disposition de la Commission nationale pour la protection des données (ci-après, la « CNPD »), sans préjudice de l'obligation au secret professionnel visée à l'article 7.

(4) Le CAA informe les personnes concernées que leurs données à caractère personnel ont fait l'objet d'un traitement si une procédure administrative ou une enquête a été menée à leur encontre ou si ces personnes ont figuré comme tiers dans une procédure administrative ou cette enquête, y compris dans les actes préparatoires, qui a été classée sans qu'une décision n'ait été prise par le CAA, à moins que ces informations ne violent le secret professionnel visé à l'article 7. L'information leur est fournie sur un support adéquat au plus tard dans les deux mois suivant le classement de la procédure ou de l'enquête.

(5) En cas de limitation des droits de la personne concernée ou de ses propres obligations, le CAA informe la personne concernée de la possibilité d'introduire une réclamation auprès de la CNPD, conformément à l'article 77 du Règlement (UE) 2016/679, à moins que ces informations ne risquent de nuire à la finalité du ou des traitements et de la limitation, notamment lorsque ces informations violent le secret professionnel auquel est tenu le CAA en application de l'article 7, ou lorsque ces informations empêchent le CAA de poursuivre une procédure administrative ou juridictionnelle à laquelle le CAA est partie.

(6) Sans préjudice du droit de réclamation auprès de la CNPD, le CAA informe la personne concernée de la possibilité de former un recours juridictionnel, à moins que cette information par le CAA ne risque de nuire à la finalité du ou des traitements et de la limitation, que cette information viole le secret professionnel auquel est tenu le CAA en application de l'article 7 ou que cette information empêche le CAA de poursuivre une procédure administrative ou juridictionnelle à laquelle le CAA est partie.

(7) Le CAA procède à une vérification régulière de ses systèmes informatiques et procédures internes afin de garantir la conformité du traitement des données à caractère personnel et des limitations aux droits de la personne concernée avec les dispositions du Règlement (UE) 2016/679.

(8) Les données à caractère personnel traitées conformément à la présente loi sont conservées aussi longtemps que nécessaire à l'exercice par le CAA de ses compétences légales.

Art. 13-9 – ***Exercice des droits par la personne concernée en cas de limitation des droits de la personne concernée***

(1) En cas de limitation des droits de la personne concernée en vertu des articles 13-3 à 13-7, les droits limités ou différés de la personne concernée peuvent être exercés par la CNPD, sans préjudice du secret professionnel du CAA prévu à l'article 7.

(2) Le CAA informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la CNPD en application du paragraphe 1er, sauf si cette information nuit à la finalité du ou des traitements et de la limitation ou lorsque cette information viole le secret professionnel du CAA prévu à l'article 7 ou empêche le CAA d'agir ou de se défendre dans une procédure administrative ou juridictionnelle.

(3) Lorsque le droit visé au paragraphe 1er est exercé, la CNPD peut communiquer à la personne concernée le résultat de ses investigations, à moins que cette information ne risque de nuire à la finalité du ou des traitements et de la limitation, que cette information viole le secret professionnel auquel est tenu le CAA en application de l'article 7 ou que cette information empêche le CAA de poursuivre une procédure administrative ou juridictionnelle dans laquelle le CAA est partie. Le cas échéant, la CNPD informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. Elle informe également la personne concernée de son droit de former un recours juridictionnel. »

3° La liste des règlements à l'annexe III de la même loi est complétée par une référence au Règlement (UE) 2016/679 de la teneur suivante :

« « Règlement (UE) 2016/679 » : 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) ».

Art. III. 1° A l'article 105 de la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement, il est ajouté un nouveau paragraphe 17, libellé comme suit :

« (17) Les limitations et garanties prévues aux articles 16-2 à 16-9 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier sont également applicables dans le contexte de l'exécution des missions légales du FRL. »

2° A l'article 154 de la même loi, il est ajouté un nouveau paragraphe 13, libellé comme suit :

« (13) Les limitations et garanties prévues aux articles 16-2 à 16-9 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier sont également applicables dans le contexte de l'exécution des missions légales du FGDL. »

*

COMMENTAIRE DES ARTICLES

Observations préliminaires

Le texte du projet de loi a pour but d'introduire dans la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier (la « Loi CSSF») et la loi modifiée du 7 décembre 2015 sur le secteur des assurances (la « LSA ») des limitations facultatives visant à restreindre la pleine application de certaines dispositions du 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 (ci-après, le « Règlement (UE) 2016/679 »). Les limitations facultatives prévues dans le présent projet de loi sont sans préjudice de l'application des dérogations prévues dans le Règlement (UE) 2016/679.

Il doit être souligné que selon le considérant 31 et l'article 4, point 9, du Règlement (UE) 2016/679, les autorités publiques telles que notamment les autorités administratives indépendantes ou les autorités des marchés financiers responsables de la réglementation et de la surveillance des marchés de valeurs mobilières, ne devraient pas être considérées comme des « destinataires » si elles reçoivent des données à caractère personnel qui sont nécessaires pour mener une enquête particulière dans l'intérêt général, conformément au droit de l'Union européenne ou au droit d'un Etat membre. Il en va ainsi, par exemple, des informations transmises par la Banque centrale européenne à la CSSF dans le cadre de l'exercice de ses missions de surveillance prudentielle sur base du règlement (UE) 2014/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit.

Toutefois, sous l'angle du Règlement (UE) 2016/679, la CSSF et le CAA peuvent figurer non seulement comme « destinataires » (article 4, point 9 du Règlement (UE) 2016/679), mais aussi comme « responsable du traitement » (article 4, point 7 du Règlement (UE) 2016/679).

Il est toutefois à noter qu'en vertu des dispositions de l'article 4, point 9, du Règlement (UE) 2016/679, la CSSF et le CAA ne seront pas considérés comme « destinataires » lorsqu'ils sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission

d'enquête particulière conformément au droit de l'Union européenne ou d'un Etat membre[1]. Par conséquent, les dispositions du présent projet de loi se rapportant à la qualité de « destinataire » ne devraient pas trouver application dans ces cas particuliers. Cela devrait s'entendre sans préjudice des garanties minimales exigées par le Règlement (UE) 2016/679 en matière de protection des données à caractère personnel et reprises dans le considérant 31 dudit règlement, qui retient que dans un tel cas « *Le traitement des données à caractère personnel par les autorités publiques en question devrait être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement.* » Selon l'approche française retenue par la loi Informatique et Libertés modifiée du 6 janvier 1978[2], les autorités publiques revêtiraient alors la qualité de « tiers autorisés », notion qui désigne l'autorité habilitée à demander la communication des données personnelles au responsable de traitement parce qu'un texte l'y autorise. Ainsi, le « tiers autorisé » bénéficie d'une habilitation lui permettant d'obtenir la communication des données, sous réserve de remplir certaines conditions[3].

Le présent projet de loi prend en considération les travaux préparatoires des projets de loi n°7168 et n°7184 et, dans le contexte des travaux préparatoires du projet de loi n°7250 visant à introduire des limitations aux dispositions du Règlement (UE) 2016/679 en matière fiscale, il tient spécialement compte de l'avis de la Commission nationale pour la protection des données (la « CNPD ») du 29 mars 2018 ainsi que de l'avis du Conseil d'Etat du 8 mai 2018. Au niveau international, il tient principalement compte du texte du « *Datenschutz- Anpassungs- und -Umsetzungsgesetz (DSAnpUG-EU)* » allemand et de ses travaux préparatoires, ainsi que des nouvelles dispositions introduites dans l'« *Abgabenordnung* » allemande à travers l'article 17 du « *Gesetz zur Änderung des Bundesvorsorgungsgesetzes und anderer Vorschriften* », qui adopte certaines limitations à l'application du Règlement (UE) 2016/679 dans le contexte de l'« *Abgabenordunung* » allemande à partir du 25 mai 2018. Ces derniers textes allemands ont servi d'inspiration au présent texte. La prise en compte de l'« *Abgabenordnung* » est motivée par le fait qu'elle contient entre autres un corps complet de règles de procédures administratives et que les limitations facultatives prévues au Règlement (UE) 2016/679 s'appliquent dans un domaine très spécifique, dans lequel il existe une obligation rigoureuse en matière de secret professionnel qui pèse sur l'administration (« *Steuergeheimnis », § 30 Abgabenordnung*). De plus, les dispositions en question de l'« *Abgabenordnung* » allemande en vigueur à partir du 25 mai 2018 présentent un certain niveau de précision. D'autre part, le texte a pris en compte le texte et les travaux préparatoires du projet de loi français relatif à la protection des données personnelles. Par ailleurs, le présent projet de loi tient également compte du *Gesetzesentwurf der Bundesregierung – Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU), dans sa version du 7 septembre 2018*.[4]

La question d'une éventuelle limitation des droits et des obligations du Règlement (UE) 2016/679 se pose principalement dans le contexte de l'exercice des missions de surveillance de la CSSF et du CAA, et plus particulièrement dans le cadre des contrôles et procédures prudentielles (préventives) ou des enquêtes et procédures de sanction (punitives). Ces missions de la CSSF et du CAA sont établies par les lois sectorielles du secteur financier qui prévoient que la CSSF et le CAA, respectivement, sont

---

1 A titre d'exemple, la CSSF ne devrait pas être considérée comme « destinataire » si elle requiert des informations dans les cas suivants :
- en vertu de l'article 7(3), al. 2 LSF ou de l'article 19(4), al. 2 LSF ;
- en vertu de l'article 44-2 LSF (coopération entre le Luxembourg et les autres Etats membres de l'Union européenne) ;
- en vertu de l'article 44-3 LSF (coopération entre le Luxembourg et les pays tiers) ;
- en vertu de l'article 59-51 LSF (échange d'informations confidentielles avec les pays tiers).

2 Le texte de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 n'aborde pas ces notions.

3 A titre d'exemple, la Commission Nationale de l'Informatique et des Libertés pose les conditions suivantes pour qu'un « tiers autorisé » puisse obtenir des informations contenues dans un fichier :
- sa demande doit être écrite et préciser le texte législatif justifiant la demande ;
- sa demande doit viser des personnes nommément identifiées ou identifiables (le tiers autorisé ne peut pas avoir accès à l'intégralité d'un fichier) ;
- sa demande doit être ponctuelle ;
- sa demande doit préciser les catégories de données auxquelles il souhaite accéder.

Consultable sur le site : https://www.cnil.fr/fr/cnil-direct/question/649

4 Consultable sur le site http://dipbt.bundestag.de/dip21/brd/2018/0430-18.pdf

les autorités (nationales) compétentes et qu'à ce titre, elles doivent veiller à la bonne application de ces lois. Très largement sous l'impulsion du cadre normatif européen, lesdites lois, au gré de leurs modifications, attribuent toujours plus de compétences aux autorités de surveillance. Cela va de pair avec le renforcement de leurs pouvoirs d'intervention, de leurs instruments et moyens d'enquête ainsi que de leur pouvoir de prononcer des sanctions (de plus en plus lourdes). Ce cadre normatif prévoit ainsi que la CSSF et le CAA peuvent prendre des mesures d'une certaine gravité à l'égard de leurs destinataires. D'une part, en ce qui concerne les sanctions administratives, la CSSF et le CAA peuvent (notamment) infliger des amendes administratives, des blâmes, ou encore des interdictions professionnelles d'une envergure plus ou moins importante. D'autre part, la CSSF et le CAA peuvent décider des mesures de police administrative ou des mesures prudentielles dans un but de prévention des risques pour le système financier, consistant notamment en des retraits d'agrément ou retraits de la liste officielle des entités surveillées, des décisions constatant qu'une personne ne répond pas à la condition de l'honorabilité professionnelle ou encore des restrictions au profil de risque des banques.

En l'absence de procédure administrative contradictoire spécifique dans les domaines de compétences de la CSSF et du CAA, ces derniers appliquent les dispositions contenues dans le Règlement grand-ducal du 8 juin 1979 relatif à la procédure à suivre par les administrations relevant de l'Etat et des communes (dit « Règlement PANC ») pour mener une enquête contradictoire et pour prendre les décisions administratives. Face à la complexité grandissante et l'internationalisation de plus en plus poussée des activités surveillées du secteur financier, et considérant la fréquence de modification et la technicité croissantes des règles de droit applicables, ces procédures et enquêtes administratives sont elles-mêmes complexifiées et demandent la prise en compte et l'évaluation d'un ensemble d'informations provenant de sources différentes, qui peuvent concerner tant des personnes morales que des personnes physiques.

Il importe aussi de préciser que même si la CSSF et le CAA surveillent majoritairement des personnes morales (de droit luxembourgeois ou de droit étranger, en cas de succursales par exemple), les personnes physiques entrent également dans leur périmètre de compétences. Dans la quasi-totalité des cas, ces « personnes concernées » au titre de la réglementation sur la protection des données personnelles sont des personnes physiques ayant un lien administratif avec la CSSF ou le CAA en raison de leurs activités professionnelles : il s'agit ainsi principalement de personnes physiques agissant au sein d'entités surveillées dans des fonctions-clés et dont l'expérience et l'honorabilité professionnelles sont appréciées par la CSSF ou le CAA. Les données à caractère personnel sont non seulement traitées pendant la phase de l'instruction de leur demande d'agrément, mais aussi pendant la surveillance continue des entités (et de leurs dirigeants). D'autre part, la CSSF et le CAA peuvent aussi être amenés à traiter des données à caractère personnel de personnes non agréées et étrangères au secteur financier. Tel est notamment le cas en matière de répression administrative de certains abus de marché au titre de la loi modifiée du 23 décembre 2016 relative aux abus de marché, en matière de réclamations de clients d'entités du secteur financier (voir par exemple l'article 58 de la loi modifiée du 5 avril 1993 relative au secteur financier), en matière de procédures ou d'enquêtes administratives, où des personnes autres que celles ayant « un lien administratif » de la CSSF peuvent rentrer dans le périmètre des compétences et des pouvoirs de l'autorité (voir par exemple les membres du personnel d'une entité surveillée, en vertu de l'article 53 de la loi modifiée du 5 avril 1993 précitée).

Ainsi, en pratique, la CSSF et le CAA collectent les données à caractère personnel directement dans le contexte des différents *reportings* prudentiels ou dans le contexte d'autres déclarations/formulaires obligatoires, en cas de transmission par une personne concernée ou par une autre personne en vertu d'une disposition légale. De telles données peuvent également être transmises par ou recueillies auprès de la personne concernée ou d'une autre personne suite à l'exercice d'un pouvoir administratif de la CSSF ou du CAA, par exemple dans le cadre d'une demande d'information et de renseignement.

C'est dans ce contexte que l'application des dispositions du Règlement (UE) 2016/679 (articles 13 et suivants) relatives entre autres à la transmission d'informations, respectivement au droit à l'obtention par la personne concernée de certaines informations (informations visant la finalité du traitement de données à caractère personnel, la nature des données traitées, les personnes auxquelles les informations sont transmises) pourra, le cas échéant, nécessiter une limitation de certains droits des personnes concernées ou d'obligations dans le chef de la CSSF et du CAA pour assurer la satisfaction effective de certaines considérations d'intérêt général supérieures à l'intérêt privé de la personne concernée. Il faut en effet assurer que la CSSF et le CAA puissent toujours, à l'avenir, mener efficacement des enquêtes ou des procédures administratives, y compris des actes préparatoires, et ce pour assurer

l'application effective des lois sectorielles du secteur financier, dans le but, notamment, d'assurer la bonne réputation du secteur financier luxembourgeois et européen, ainsi que la stabilité financière[5] dont découle le bon fonctionnement du marché intérieur (tel que défini à l'article 3 du Traité sur l'Union européenne).

Si le Règlement (UE) 2016/679 permet de limiter par des mesures nationales les droits de la personne concernée et les obligations du responsable du traitement, c'est-à-dire de la CSSF ou le CAA (et de leurs sous-traitants) conformément à l'article 23 du Règlement (UE) 2016/679, ce n'est qu'à la condition que les limitations respectent certains critères spécifiques dont l'objectif est de garantir et de maintenir, malgré la limitation, un haut niveau de protection.

Les limitations qui peuvent être imposées par la CSSF et le CAA visent à garantir les objectifs énumérés à l'article 23, paragraphe 1er, lettres e) et h), voire pour certaines compétences de la CSSF et du CAA la lettre d) et j) du Règlement (UE) 2016/679. En même temps, les limitations ne peuvent être mises en œuvre que si des garanties particulières sont données pour compenser les limitations (article 23, paragraphe 2 du Règlement (UE) 2016/679 ; articles 16-8 de la Loi CSSF et 13-8 de la LSA introduits par le présent projet).

Il reste à remarquer qu'à l'heure actuelle, le degré de précision et l'étendue des limitations ainsi que des garanties à donner à la personne concernée sont certes précisés par la jurisprudence, mais il n'en demeure pas moins que les dispositions du Règlement (UE) 2016/679 laissent ouvertes certaines questions. Ainsi, par exemple, la doctrine allemande considère que les textes nationaux qui prévoient les limitations choisies ne devraient pas refléter toutes les conditions et protections prévues à l'article 23, paragraphe 2, du Règlement (UE) 2016/679, en raison de la formulation prévue dans ce paragraphe (« *dispositions spécifiques relatives, au moins, le cas échéant* »). De même, la récente loi irlandaise en matière de protection des données reflète également une certaine marge de discrétion et d'interprétation tant dans la configuration des limitations que dans les garanties à octroyer en contrepartie

Il est enfin important de souligner que le terme de « *personne concernée* » utilisé dans le texte du présent projet de loi se réfère à la notion qui lui est attribuée à l'article 4, point 1, du Règlement (UE) 2016/679, c'est-à-dire à la personne physique identifiée ou identifiable à laquelle se rapportent les données à caractère personnel en cause. Cette approche a d'ailleurs été reprise dans le texte allemand précité.

Article Ier

Une limitation importante des droits de la personne concernée réside dans le secret professionnel de la CSSF, qui est consacré à l'article 16 de la Loi CSSF, et dont la violation est pénalement sanctionnée par application des dispositions de l'article 458 du Code pénal. Cette obligation au secret ne peut être levée que dans certains cas strictement délimités par le législateur, et prévus dans le texte-même de l'article 16 précité. Il a été rappelé par le juge européen que le secret professionnel des autorités de surveillance est une nécessité fondamentale dans l'intérêt général à la stabilité financière[6].

Selon les lois sectorielles luxembourgeoises régissant les différentes activités du secteur financier, la CSSF est désignée comme autorité compétente qui veille au respect de ce cadre réglementaire. Dans ce contexte, la CSSF s'est vu attribuer des compétences et des pouvoirs en matière de surveillance, de

---

5 Nous rappellerons l'absolue nécessité pour la CSSF, en tant qu'autorité de surveillance, de garantir l'intégrité et la stabilité financières, s'agissant d'objectifs prééminents du droit de l'Union européenne (Cour de justice de l'Union européenne, arrêt *Pringle* du 27 novembre 2012, affaire C-370/12) dont la réalisation dépend de l'exercice efficace, par la CSSF, de ses pouvoirs d'enquêtes et de sanction (ce qui inclut la coopération sur un plan européen et international).

6 Voy. la référence en note de bas de page n°5, ainsi que l'arrêt de la Cour de justice de l'Union européenne Altmann du 12 novembre 2014 (aff. C-140/13). Cette décision, rendue dans le cadre juridique de la directive 2004/39/CE du Parlement européen et du Conseil du 21 avril 2004 (dite « MIFID »), précise dans ses motifs que « *l'article 54, paragraphes 1 et 2, de la directive 2004/39/CE du Parlement européen et du Conseil, du 21 avril 2004, concernant les marchés d'instruments financiers, modifiant les directives 85/611/CEE et 93/6/CEE du Conseil et la directive 2000/12/CE du Parlement européen et du Conseil et abrogeant la directive 93/22/CEE du Conseil, doit être interprété en ce sens qu'une autorité nationale de surveillance peut invoquer, dans le cadre d'une procédure administrative, l'obligation de garder le secret professionnel à l'encontre d'une personne qui, en dehors d'un cas relevant du droit pénal ou d'une procédure civile ou commerciale, lui a demandé l'accès à des informations concernant une entreprise d'investissement qui se trouve désormais en liquidation judiciaire, quand bien même le principal modèle commercial de cette entreprise aurait consisté dans une fraude de grande ampleur visant à escroquer sciemment les investisseurs et plusieurs des responsables de ladite entreprise auraient été condamnés à des peines privatives de liberté.* »

contrôle et d'enquête en vue d'investiguer si les entités surveillées respectent effectivement le cadre réglementaire qui leur est applicable, pour les sanctionner si tel n'est pas le cas ou, lorsque des dispositions pénales sont prévues, pour dénoncer les faits au Parquet. Ainsi, à titre d'exemples (non exhaustifs), la loi modifiée du 5 avril 1993 relative au secteur financier contient des dispositions attribuant des pouvoirs en matière de surveillance et d'enquête à la CSSF agissant en tant qu'autorité de surveillance prudentielle (Partie II, spécialement Chapitre IV) ainsi qu'à la CSSF agissant en sa capacité d'autorité de résolution (Partie IV). Dans la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif, c'est essentiellement le Chapitre 20 dédié à l'organisation de la surveillance qui a trait aux compétences et pouvoirs de la CSSF. De même, dans la loi modifiée du 23 décembre 2016 relative aux abus de marché, le législateur a attribué des pouvoirs d'investigation très larges à la CSSF. Ainsi, l'exercice de ses compétences légales permet à la CSSF de mettre en œuvre des contrôles sur place, de collecter et de demander des informations et d'imposer des mesures prudentielles ou de police administrative, ainsi que des sanctions administratives. Pour mener à bien ses attributions dans l'intérêt général, et spécialement en vue d'assurer la stabilité du secteur financier et donc de maintenir la confiance du public dans le secteur financier, il est essentiel (notamment) pour éviter des entraves aux enquêtes que certains droits que les personnes concernées tirent du Règlement (UE) 2016/679, ou certaines obligations imposées à la CSSF, soient limités ou retardés pendant un délai suffisant afin que l'autorité compétente puisse effectivement exécuter ses attributions légales.

Les restrictions (qui peuvent être des limitations ou simplement un retard de l'exercice des droits, respectivement de l'exécution des obligations de la CSSF) n'existent que dans le cadre de l'exécution de prérogatives de puissance publique, donc dans l'exécution des missions de la CSSF, et spécialement dans le contexte de mesures d'enquête et d'application de la loi (*enforcement*) et les missions d'investigation.

L'exercice effectif, par la CSSF, de la coopération et de l'échange d'informations avec des autorités compétentes d'autres Etats membres de l'Union européenne ou de pays tiers, ainsi qu'avec des organisations ou autorités internationales ou européennes, requiert également que certains droits que les personnes concernées tirent du Règlement (UE) 2016/679 ou certaines obligations dans le chef de la CSSF soient limités ou retardés pendant un délai maximal, afin que la CSSF puisse effectivement exécuter ses attributions légales en la matière. Sont ainsi concernées, par exemple :

– la coopération horizontale entre la CSSF et ses homologues des autres Etats membres de l'Union européenne, sur base (notamment) des normes de l'Union européenne transposées en droit national ou directement applicables ;
– dans l'intérêt de la protection des investisseurs et des déposants ainsi que de la stabilité financière, la coopération internationale prévue au dernier alinéa de l'article 16 de la Loi CSSF qui permet à la CSSF, par exemple, de transmettre certaines informations couvertes par le secret professionnel à une autorité d'un Etat tiers, ou bien à des institutions internationales telles que le Fonds monétaire international (FMI) ou la Banque des règlements internationaux (BRI), si les conditions posées par la disposition sont remplies (notamment une obligation de confidentialité réciproque).

De même, la CSSF peut être amenée à transmettre des données à caractère personnel à des autorités nationales (notamment au Procureur d'Etat, en vertu de l'article 23 du Code de procédure pénale).

Commentaire du point 1°

La disposition introduite par le point 1° clarifie que la CSSF est autorisée à procéder à la collecte et au traitement des données à caractère personnel. La disposition souligne la licéité du traitement des données à caractère personnel par la CSSF, sans préjudice des cas visés à l'article 6 du Règlement (UE) 2016/679. Ce sont les lettres c) et e) de l'article 6, paragraphe 1er, ainsi que la lettre e) de l'article 23, paragraphe 2, du Règlement (UE) 2016/679 qui sont concrétisées ici. La disposition renvoie aux articles 2 à 2-3 et aux lois sectorielles y répertoriées. La précision sert donc à garantir la conformité avec la jurisprudence de la Cour européenne des droits de l'Homme, notamment les critères d'accessibilité et de prévisibilité, et *in fine* de précision de la Loi. En effet la Cour de Strasbourg exige, selon une jurisprudence constante rendue au visa de l'article 8 de la Convention, de tenir compte tant de la nécessité de protéger la vie privée des individus que de la nécessité de prendre en compte les limitations ou restrictions imposées par les Etats : la Cour accepte de telles limitations tout en exigeant qu'elles soient prévues dans une loi accessible et prévisible – c'est-à-dire formulée avec une précision suffisante pour permettre à toute personne d'adapter son comportement, le cas échéant sur base d'une assistance

appropriée[7] – dans ses effets et quant à ses répercussions[8], qu'elles poursuivent un but légitime et qu'elles soient nécessaires dans une société démocratique. Le droit de l'Union européenne semble suivre cette approche[9]. Pour des raisons de lisibilité, de facilité rédactionnelle et donc d'accessibilité de la règle de droit[10], et pour *in fine* valider le test d'attente légitime qu'impose la Cour de Strasbourg, cette disposition est inscrite dans la Loi CSSF, et non dans chacune des lois sectorielles qui réglemente chaque secteur d'activités sur la place financière et qui attribue des compétences et des pouvoirs à la CSSF (auxquels il est renvoyé à travers les articles 2 à 2-3).

Commentaire du point 2°

Article 16-1

Le paragraphe 1er du nouvel article 16-1 est proposé dans le contexte de l'article 6, paragraphe 3, second alinéa, du Règlement (UE) 2016/679. Ce sont essentiellement les indications visées sur les papiers d'identités de la personne concernée, les données normalement inscrites sur un *curriculum vitae*, certaines indications sur le patrimoine (numéros de compte, solde du compte, etc.) ainsi que les données sur les antécédents personnels et professionnels de la personne concernée qui sont traitées. Les informations sont principalement transmises par les personnes concernées elles-mêmes, ou par des intermédiaires (avocats, …) agissant pour elles, entre autres pour effectuer les démarches administratives auprès de la CSSF. Par ailleurs, les données à caractère personnel peuvent également être collectées en vue d'un traitement auprès de tiers : tel est le cas si la CSSF procède à une enquête sur place ou demande simplement des renseignements sur une personne donnée à une entité surveillée.

Le paragraphe 2 souligne l'importance du secret professionnel dans l'exécution des missions de la CSSF. Le secret professionnel est une nécessité pour assurer le bon fonctionnement de la surveillance prudentielle et des marchés financiers. Le traitement des données à caractère personnel est ainsi sans préjudice de l'article 16 de la Loi CSSF qui consacre le secret professionnel et sanctionne ses violations par référence à l'article 458 du Code pénal (tenant à l'ordre public luxembourgeois, cette disposition doit nécessairement primer). Ainsi, des informations confidentielles qui contiennent des données à caractère personnel ne peuvent pas être divulguées à des tiers en dehors des cas d'exception relatifs au secret professionnel. Toutefois il est bien clair que le secret professionnel ne peut pas être détourné de sa finalité pour empêcher dans tous les cas l'exercice légitime par la personne concernée de ses droits fondamentaux tirés du Règlement (UE) 2016/679.

Les limitations aux droits de la personne concernée et aux obligations de la CSSF qui sont prévues dans les articles subséquents s'appliquent lorsque la CSSF en tant que personne morale de droit public est engagée par la direction, le CPDI ou par le conseil de résolution. A cet égard, la limitation aux droits de la personne concernée ou aux obligations dans le chef de la CSSF doit être nécessaire pour les fins auxquelles il est renvoyé compte tenu du cadre concret ; cette limitation doit en outre respecter le principe de proportionnalité.

---

7 Les juges ont, à de nombreuses reprises, rappelé aux Etats membres de la Convention la nécessité de rédiger les lois « *avec assez de précision pour permettre à toute personne, en s'entourant au besoin de conseils éclairés, de régler sa conduite.* » Voy. notamment Cour européenne des droits de l'Homme, 14 mars 2002, *Gaweda contre Pologne*, Req. n°26229/95 ; voy. également Cour européenne des droits de l'Homme, *Silver et autres c. Royaume-Uni*, n° 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983 (§88).

8 Il s'agit d'un test d'« attente légitime » ou d'« aspiration raisonnable » à la vie privée. Voy. par exemple Cour européenne des droits de l'Homme, *Iordachi et autres contre Moldavie*, n°25198/02, 10 février 2009 (§50).

9 « *L'exigence de prévisibilité a trouvé une expression particulière dans le droit de la protection des données qui impose que tout traitement de données soit lié à des fins déterminées, comme l'exige expressément l'article 8, paragraphe 2, de la charte* » (conclusions de l'avocat général *Kokott* rendues le 18 juillet 2007 dans l'affaire *Promusicae contre Telefónica de España SAU*, C 275/06, §53) ; « *La situation en cause au principal est, par ailleurs, susceptible de relever tant de l'article 10 de la directive 95/46 que l'article 11 de celle ci. En effet, et ainsi qu'il ressort des développements qui précèdent, le traitement loyal par l'ANAF des données personnelles des requérants au principal impliquait que cette dernière les informât, notamment, de la transmission de ces données à la CNAS, conformément à l'article 10, sous c), de la directive 95/46. Par ailleurs, le traitement par la CNAS des données transmises par l'ANAF impliquait également que lesdits requérants fussent à tout le moins informés des finalités dudit traitement ainsi que des catégories de données concernées, conformément à l'article 11, paragraphe 1, sous b) et sous c), de la directive 95/46* » (conclusions de l'Avocat général Cruz Villalón présentées le 9 juillet 2015 dans l'affaire C 201/14, §63). Voy., plus récemment, CJUE, *Maximilian Schrems contre Data Protection Commissionner*, aff. C-362/14 du 6 octobre 2015.

10 Qui constitue le corollaire du droit fondamental à une protection juridictionnelle effective, tel que garanti par l'article 47 de la Charte des droits fondamentaux de l'Union européenne et les articles 6 et 13 de la Convention européenne des droits de l'Homme.

Article 16-2

L'article 16-2 permet explicitement à la CSSF d'effectuer un traitement de données à caractère personnel à des fins autres que celles pour lesquelles les données ont été collectées, et ce dans un cadre juridique prévisible et sécurisé, prévu par le droit national. Cette disposition est donc sans préjudice des lettres a) à e) du paragraphe 4 de l'article 6 du Règlement (UE) 2016/679. L'article 23 du DSAnpUG-EU allemand et l'article 29c de l'« *Abgabenordnung* » allemande qui sont entrés en vigueur le 25 mai 2018 ont servi d'inspiration à la présente disposition. Dans ces deux textes, un traitement à une autre fin que celle pour laquelle les données ont été collectées est encadré par des critères à respecter par le responsable du traitement.

Article 16-3

L'article 16-3 précise les situations dans lesquelles la CSSF peut limiter ou différer la fourniture d'informations dans le cadre de l'article 13 du Règlement UE 2016/679.

Pour respecter le principe de proportionnalité, le texte (des différentes limitations) prévoit que la CSSF peut limiter ou retarder en tout ou en partie les droits (ou ses propres obligations) découlant du Règlement (UE) 2016/679 ; la limitation ou le retard ne peuvent donc concerner uniquement les éléments (par exemple certaines des informations à fournir) qui sont nécessaires et adéquats pour atteindre la finalité justifiant la limitation ou le retard. Il n'y a pas de limitation pure et simple de tout le droit mais, le cas échéant, de certains éléments du droit, selon le cas spécifique et concret. Ce cas spécifique et concret, par exemple une enquête administrative, peut également justifier que pendant un certain délai, tous les éléments du droit ou toutes les informations soient limités ou retardés. Les limitations peuvent donc concerner certains droits ou tous les droits en fonction du cas concret. Pour chaque cas précis, il s'agit d'affiner la restriction en vue de limiter au maximum la restriction apportée aux droits fondamentaux de la personne concernée à ce qui est nécessaire pour garantir les objectifs poursuivis par la limitation. Par conséquent, la CSSF devra mettre en œuvre des limitations en tenant compte de toutes les spécificités du cas concret, en fonction des circonstances spécifiques, en respectant le principe de proportionnalité.

Ainsi, par principe la personne concernée ne peut se voir limiter ses droits, sauf s'il existe un motif impérieux indiqué dans les lettres a) à f).

Les limitations prévues dans le présent projet de loi doivent être lues dans le contexte de l'article 23, paragraphe 1er, en particulier les lettres e) et h) du Règlement UE 2016/679. Ainsi, les limitations sont motivées dans la mesure où elles poursuivent des objectifs importants d'intérêt public général de l'Union européenne ou d'un Etat membre (lettre e), en ce comprises spécifiquement les tâches attribuées à la CSSF par les articles 2 à 2-3 de la Loi CSSF, c'est-à-dire notamment la surveillance prudentielle du secteur financier et la surveillance des marchés. Dans ce contexte, la CSSF dispose de pouvoirs étendus et elle poursuit « *une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, …* » (lettre h).

Dans un texte général et abstrait, il est impossible de fournir tous les cas de manière détaillée et de préciser pour chacun les éventuelles limitations possibles. Toutefois, il est évident que la ou les limitations à certains droits ou obligations viseront principalement la communication ou le droit d'accès à toutes les informations ou seulement à une partie de celles-ci (limitation partielle), dans un contexte où la communication serait contreproductive à la finalité d'intérêt général des missions de la CSSF. Il apparaît donc que la détermination concrète et précise de l'étendue de la limitation ne pourra se faire qu'en fonction des circonstances concrètes de chaque cas apprécié individuellement, alors qu'un texte général ne pourra jamais parfaitement refléter toutes ces circonstances. D'autre part, une limitation peut aussi se concrétiser par un retard dans la communication de ces informations pendant la durée nécessaire à atteindre la finalité qui justifie la limitation des droits. La CSSF aura recours à la mesure la moins contraignante.

Les lettres a) à f) reflètent les dispositions de l'article 23, paragraphe 1er, du Règlement (UE) 2016/679 et sont inspirées dans une certaine mesure des commentaires du Règlement (UE) 2016/679 élaborés par la doctrine allemande précitée. De même, les dispositions de l'« *Abgabenordnung* » allemande (en particulier les §§ 29 a et s.) en vigueur à partir du 25 mai 2018 ont servi d'inspiration. Ainsi, l'article détermine avec une précision similaire au texte allemand de l'« *Abgabenordnung* » les cas dans lesquels une limitation peut être justifiée (voir notamment les §§ 29a et suivants de l'« *Abgabenordnung* »). Une autre source d'inspiration a été le *Gesetzesentwurf der Bundesregierung zum Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz* EU (2. DSAnpUG-EU) dans sa version du 7 septembre 2018 précité.

Ce projet adapte les dispositions de certains articles de diverses lois allemandes, dont le *Kreditwesengesetz* (article 91) et le *Finanzdienstleistungsaufsichtsgesetz* (article 93).

La lettre a), dans son libellé proche de celui qui a été proposé par la CNPD dans son avis du 29 mars 2018, est inspiré de l'article 3, paragraphe 7, de la loi belge modifiée du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Ainsi, cette disposition permet de limiter les droits ou obligations si leur plein exercice compromet ou entrave dans un cas concret l'exercice de procédures administratives ou d'enquêtes ou leurs actes préparatoires. La formulation tient compte de la nature variée de l'intervention de la CSSF, dans la mesure où elle peut imposer des mesures de sanction administrative (amendes, interdiction professionnelle), des mesures de police administrative (décision sur l'honorabilité professionnelle, sur l'expérience professionnelle des dirigeants) voire des mesures prudentielles (assises financières, décisions sur la distribution des gains…). Ces mesures impliquent le respect de règles procédurales (notamment celles de la procédure administrative non contentieuse, à la lumière des droits procéduraux issus du droit de l'Union européenne et du droit conventionnel) et nécessitent en principe des actes préparatoires et une enquête. Ces procédures ou enquêtes sont toujours exclusivement diligentées dans l'intérêt général, dans la mesure où l'article 20, paragraphe 1er de la Loi CSSF précise que la CSSF agit exclusivement dans l'intérêt général. L'application de cette disposition demande dès lors une appréciation concrète et la limitation envisagée doit réussir le test de la proportionnalité. Il faut aussi que l'intérêt public et général à ne pas communiquer soit suffisamment clair et prévale sur les intérêts de la personne individuelle concernée. La disposition pourra dès lors trouver application, le cas échéant, pour ne pas entraver une enquête ou des actes préparatoires à une enquête que la CSSF diligente lorsqu'elle suspecte la violation d'une disposition législative ou règlementaire dont elle assure le respect dans l'intérêt général.

La lettre b) constitue une autre limite au plein exercice de droits ou d'obligations qui se justifie par des facteurs externes à la CSSF. Ici, la limitation est principalement justifiée par l'impact d'une communication de certaines informations à la personne concernée sur le bon fonctionnement des marchés ou la stabilité financière, voire la sécurité publique et l'ordre public en cas de crise importante, si une telle information est concrètement de nature à créer ce risque (par exemple un « *bank run* »). Il est ainsi rappelé que la stabilité du secteur financier constitue un objectif d'intérêt général du droit de l'Union européenne comme l'a précisé la Cour de justice de l'Union européenne (« CJUE ») dans l'arrêt *Pringle* précité.

La lettre c) protège les intérêts légitimes de la CSSF. Dans des cas concrets et si tel est nécessaire, le plein exercice des droits ou des obligations découlant du Règlement (UE) 2016/679 peut être limité lorsque la CSSF est appelée à agir ou à se défendre dans des procédures administratives (notamment au niveau de l'Union européenne, lorsqu'il s'agit pour l'autorité nationale de se défendre dans une procédure en non-application ou en violation du droit de l'Union) ou dans des procédures juridictionnelles, qu'elles soient menées devant les juridictions administratives ou judiciaires. La disposition reflète en cela l'article 23, paragraphe 1er, lettres e), f), h) et j) du Règlement UE 2016/679 (qui visent chacune des hypothèses précises).

La lettre d) prévoit la possibilité d'invoquer une restriction si la CSSF fait notamment l'objet de procédures en non-application ou violation du droit de l'Union européenne que les autorités de surveillance européennes (ESMA, EIOPA, EBA) peuvent diligenter contre une autorité nationale de surveillance dans le cadre leurs missions prévues aux règlements qui les instituent[11].

De telles procédures dites de « *breach of Union law* »[12] peuvent être menées parallèlement à des procédures nationales devant des juridictions administratives ou civiles dans lesquelles l'autorité nationale de surveillance est partie : pour garantir l'exercice efficace par celle-ci de ses missions d'intérêt général, il y a lieu d'éviter tout risque d'interférence entre ces différentes procédures. En particulier, un tel risque se trouverait accru, en pratique, si des régimes différents quant à la limitation de l'exercice des droits ou obligations découlant du Règlement (UE) 2016/679 étaient instaurés entre les procédures administratives au niveau de l'Union européenne et les procédures juridictionnelles.

---

11 Règlement (UE) n°1093/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité bancaire européenne) ; règlement (UE) n°1094/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles) ; règlement (UE) n°1095/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des marchés financiers).

12 Voir par exemple article 17 du règlement (UE) n°1095/2010.

Il ne serait en effet pas concevable, à la fois pour garantir une surveillance efficace dans l'intérêt général et l'effet utile du Règlement (UE) 2016/679, qu'un investisseur soit incité à saisir l'Autorité européenne des marchés financiers en parallèle d'une procédure devant les juridictions nationales dans laquelle il est impliqué, dans le seul but de maximiser ses chances d'échapper aux dérogations au Règlement (UE) 2016/679 qui bénéficient à l'autorité de surveillance, et ainsi de faire valoir son droit d'obtenir tout ou partie des informations visées à l'article 13, paragraphes 1 et 2 du Règlement (UE) 2016/679.

La lettre e) aborde les exigences liées à la coopération des autorités de surveillance dans le contexte d'un secteur financier international et de plus en plus globalisé. Dans ce cadre, la CSSF est amenée à coopérer avec des autorités nationales, européennes ou étrangères. Dans certains cas, il faut assurer que l'exercice des missions d'intérêt général dans le contexte international ne puisse pas être entravé par le plein exercice des droits de la personne concernée et obligations de la CSSF découlant du Règlement (UE) 2016/679, lorsqu'il existe une communication de données à caractère personnel vers ou en provenance de ces autorités. Dans ce contexte, les droits des personnes concernées doivent également être lus dans le contexte du secret professionnel de la CSSF et des règles générales relatives à la coopération[13].

La lettre f) permet également, compte tenu des circonstances concrètes et en application du principe de proportionnalité, d'éviter la communication de ces informations à la personne concernée si des intérêts légitimes d'un tiers sont affectés par cette communication. Tel pourra par exemple être le cas pour justifier une limitation à l'article 15 du Règlement (UE) 2016/679 afin de protéger un tiers qui a révélé des informations sensibles à la CSSF (lanceur d'alerte par exemple), sans préjudice de l'application de l'obligation au secret de la CSSF.

Article 16-4

L'article 16-4 concerne des limitations à l'article 14 du Règlement (UE) 2016/679, qui concerne les informations à fournir si les données à caractère personnel n'ont pas été collectées auprès de la personne concernée. Les cas dans lesquels la restriction peut être invoquée par la CSSF sont ceux visés aux lettres a) à f) du de l'article 16-3. Pour des raisons de lisibilité et afin de ne pas allonger le texte, il est opéré par renvoi.

Article 16-5

L'article 16-5 permet à la CSSF d'apporter des restrictions au droit d'accès de la personne concernée visé à l'article 15 du Règlement (UE) 2016/679. Les dispositions prévues dans cette disposition permettent de limiter le droit fondamental de la personne concernée d'avoir confirmation d'un traitement de ses données personnel, et le cas échéant d'avoir accès à une information, notamment quant à la finalité dudit traitement et sous réserve du respect du principe de proportionnalité. Ainsi, dans les cas visés à l'article 16-3, lettres a) à f), et en vue d'une finalité visée à l'article 23, paragraphe 1er, lettres e) et h), la CSSF peut limiter ou retarder la confirmation à la personne concernée que des données à caractère personnel sont ou ne sont pas traitées, et lorsqu'elles le sont, retarder ou limiter l'accès auxdites données. La disposition permet également de limiter en tout ou en partie la fourniture des informations visées à l'article 15, paragraphes 1 et 2 du Règlement (UE) 2016/679.

Article 16-6

L'article 16-6 permet à la CSSF de restreindre le droit de la personne concernée d'obtenir de la CSSF la limitation du traitement dans les cas visés à l'article 16-3, lettres a) à f).

Article 16-7

L'article 16-7 permet à la CSSF de limiter ou de retarder le droit de la personne concernée de s'opposer au traitement des données personnelles. L'article 16-7 concrétise l'exception prévue à la seconde phrase de l'article 21 du Règlement (UE) 2016/679 qui permet de ne pas donner suite à cette demande lorsqu'il existe des motifs légitimes et impérieux pour le traitement qui doivent prévaloir sur les intérêts et les droits et libertés de la personne concernée, pour la constatation, l'exercice ou la défense de droits en justice. L'application de l'article 16-7 n'est pas automatique – comme l'article 21 du Règlement UE 2016/679 – dans la mesure où la CSSF doit démontrer que concrètement dans le cas spécifique, l'un des cas prévus à l'article 16-3, lettres a) à f), s'applique.

---

13 Voir notamment articles 44-2 LSF, 44-3 et 59-5 précités.

Article 16-8

Cette disposition prévoit les garanties que la CSSF doit prévoir en vue de compenser les limitations ou le retard de l'exercice des droits des personnes concernées ou de ses propres obligations du Règlement (UE) 2016/679.

Selon la doctrine allemande précitée, les conditions prévues à l'article 23, paragraphe 2, du Règlement UE 2016/679, ne doivent pas toutes être reflétées dans les textes nationaux, en raison de la formulation « au moins, le cas échéant ». Il y a dès lors lieu de suivre une approche qui préconise d'appliquer autant que possible ces garanties, mais en fonction des cas spécifiques des limitations.

Le paragraphe 1er prévoit une disposition qui limite les effets d'une décision de retarder l'exécution des obligations de la CSSF ou des droits de la personne concernée en cas d'événement temporaire et externe à la CSSF. Ainsi, la CSSF lève la limitation à partir du moment où la cause qui justifie la limitation a cessé d'exister ou a cessé de produire ses effets.

Le paragraphe 2 oblige la CSSF à informer la personne concernée dans le mois de la survenance de la cause qui justifie la limitation ou le retard de l'existence de la limitation ou du retard. Conformément à l'article 23, paragraphe 2, lettre h), cette obligation de transparence peut être supprimée si la communication risque de nuire à la finalité de la limitation. Tel sera notamment le cas si la communication viole le secret professionnel de la CSSF ou si elle empêche la CSSF d'agir ou de se défendre dans une procédure administrative ou juridictionnelle.

Le paragraphe 3 oblige la CSSF à consigner par écrit les motifs de fait ou de droit sur lesquels se fonde sa décision de limiter ou de différer l'exécution des droits et des obligations d'information de la personne concernée. Dans le cas où l'exercice d'un droit ou d'une obligation est différé, la CSSF indique la date à partir de laquelle le droit limité pourra à nouveau être exercé ou, à défaut de date, les circonstances qui permettront à nouveau l'exercice du droit concerné.

Sans préjudice du respect du secret professionnel de la CSSF, ces informations sont mises à la disposition de la CNPD.

Le paragraphe 4 prévoit que si une procédure administrative ou une enquête est classée sans suite, la CSSF devra informer la personne concernée que ses données ont fait l'objet d'un traitement

Le paragraphe 5 oblige la CSSF à informer la personne concernée de la possibilité d'introduire une réclamation auprès de la CNPD. Cette obligation à l'information peut être écartée si elle risque de nuire à la finalité de la limitation ce qui est par exemple le cas si elle viole le secret professionnel de la CSSF ou empêche la CSSF d'agir ou de se défendre dans une procédure administrative ou juridictionnelle.

Il est évident que lorsque la CNPD informe la personne concernée conformément à l'article 77, paragraphe 2, du Règlement UE) 2016/679, cette information ne doit pas comporter des éléments confidentiels, notamment relatives à l'état de procédures administratives ou de sanctions ainsi que sur la surveillance visant la personne concernée.

Le paragraphe 6 oblige la CSSF à informer la personne concernée de la possibilité de former un recours juridictionnel. Tout comme pour la possibilité d'introduire une réclamation auprès de la CNPD, l'obligation à l'information n'existe pas si elle risque de nuire à la finalité de la limitation.

Le paragraphe 7 prévoit une disposition qui oblige la CSSF à procéder à une revue régulière de ses systèmes pour assurer une conformité avec la réglementation, les principes et les orientations qui sont dégagés au fur et à mesure.

Le paragraphe 8 prévoit que les données à caractère personnel ne sont conservées qu'aussi longtemps que nécessaire à l'exercice par la CSSF de ses compétences légales.

Article 16-9

Le paragraphe 1er de l'article 16-9 introduit, en plus des garanties mentionnées à l'article 16-8 (sous certaines réserves), un droit d'accès indirect pour les personnes concernées, pour le cas où le droit d'accès serait limité. Cet accès indirect est effectué par la CNPD. Un tel droit d'accès indirect existait aussi dans le cadre de la loi modifiée de 2002 sur la protection des données pour garantir aux personnes concernées qu'une autorité indépendante puisse vérifier la licéité du traitement. La disposition en question se fonde sur l'avis *WP258 de l'Article 29 Working Party « Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)* » du 29 novembre 2017 qui prévoit qu'en cas de restriction des droits, les personnes concernées peuvent exercer leurs droits à travers l'autorité de contrôle nationale. Ce mécanisme de contrôle se conçoit cependant dans les limites que le secret professionnel de la CSSF pose.

Le paragraphe 2 oblige la CSSF à informer la personne concernée de la possibilité de faire exercer ses droits par la CNPD. Cette obligation à l'information peut être écartée si elle risque de nuire à la finalité de la limitation ce qui est par exemple le cas si elle viole le secret professionnel de la CSSF ou empêche la CSSF d'agir ou de se défendre dans une procédure administrative ou juridictionnelle.

Le paragraphe 3 prévoit les informations qui pourront être transmises aux personnes concernées sur les résultats de l'accès indirect.

Article II

L'article II du présent projet de loi introduit des dispositions similaires à celles commentées ci-dessus.

De la même manière que pour la CSSF, une limitation importante des droits de la personne concernée constitue le secret professionnel du CAA, qui est consacré à l'article 7 de la LSA et dont la violation est pénalement sanctionnée par application des dispositions de l'article 458 du Code pénal. Cette obligation au secret ne peut être levée que dans certains cas strictement délimités par le législateur, et prévus dans le texte de l'article 7 précité. Il a été rappelé par le juge européen que le secret professionnel des autorités de surveillance est une nécessité fondamentale dans l'intérêt général à la stabilité du secteur bancaire et financier.

Commentaire du point 1°

Cette disposition souligne la licéité du traitement des données à caractère personnel par le CAA sans préjudice des cas visés à l'article 6 du Règlement (UE) 2016/679. Ce sont les lettres c) et e) de l'article 6, paragraphe 1er, et la lettre e) de l'article 23, paragraphe 2, du Règlement (UE) 2016/679 qui sont concrétisées ici. Pour plus de détails, il est renvoyé aux propos concernant l'article Ier, point 1° du présent projet de loi.

Commentaire du point 2°

Article 13-1

Le paragraphe 1er de l'article 13-1 est proposé dans le contexte de l'article 6, paragraphe 3, second alinéa, du Règlement (UE) 2016/679. Pour plus de détails, il est renvoyé aux propos concernant l'article 16-1, paragraphe 1er, ci-dessus

Le paragraphe 2 souligne l'importance du secret professionnel dans l'exécution des missions du CAA et que le traitement des données est sans préjudice de l'article 7. Cette disposition vise principalement le fait que des informations confidentielles qui contiennent des données à caractère personnel ne peuvent pas être divulguées à des tiers en dehors des cas d'exception relatifs au secret professionnel.

Article 13-2

L'article 13-2 permet explicitement le traitement de données à caractère personnel par le CAA à des fins autres que celles pour lesquelles les données ont été collectées dans un cadre juridique prévisible et sécurisé prévu par le droit natinal. Cette disposition est donc sans préjudice des points a) à e) du paragraphe 4 de l'article 6 du Règlement (UE) 2016/679. Pour plus de détails, il est renvoyé au commentaire concernant l'article Ier, point 2° (article 16-2).

Article 13-3

L'article 13-3 prévoit les limitations que le CAA pourra mettre en œuvre dans un cas concret, en fonction des circonstances spécifiques tout en respectant le principe de proportionnalité concernant certains articles du Règlement (UE) 2016/679. Les explications fournies au niveau de l'article 16-3 sont également valables pour l'article 13-3.

Articles 13-4 à 13-7

Les articles 13-4 à 13-7 concernent les différentes limitations qui peuvent être mises en œuvre en vertu de l'article 23 du Règlement (UE) 2016/679. Pour plus de détails, il est renvoyé aux propos concernant les articles 16-4 à 16-7 ci-dessus.

Articles 13-8 à 13-9

Les articles 13-8 à 13-9 prévoient les conditions à respecter en vertu de l'article 23, paragraphe 2, du Règlement (UE) 2016/679 et la possibilité pour une personne concernée d'exercer ses droits par

l'intermédiaire de la CNPD. Les mêmes commentaires que ceux concernant les articles 16-8 à 16-9 ci-dessus s'appliquent.

Commentaire du point 3°

L'insertion de l'intitulé complet du Règlement (UE) 2016/679 à l'endroit de l'annexe III de la LSA est la suite logique du commentaire fait à l'occasion de l'introduction d'un article 13-1, paragraphe 1, dans la LSA.

Article III

Les points 1° et 2° de l'article III du projet de loi visent à introduire dans la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement une référence aux articles 16-2 à 16-9 de la Loi CSSF étant donné que les limitations et garanties prévues dans le présent projet de loi devraient également pouvoir être mises en œuvre dans le cadre des missions du FGDL et du FRL. En effet, lesdites missions peuvent, dans des cas bien délimités, également justifier une limitation des droits d'une personne concernée ou des obligations de la CSSF.

Etant donné qu'il s'agit de deux établissements publics indépendants, il est nécessaire de modifier la loi précitée de 2015 qui institue les deux fonds au niveau des articles 105 et 154. A des fins de lisibilité et de clarté du texte, il a été décidé de ne pas répliquer les articles 16-2 à 16-9 mais d'y faire référence.

*

TEXTES COORDONNES

TEXTE COORDONNE

de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier (extraits)

[…]

Section 2 : Mission et compétences de la CSSF

[…]

Art. 3. Dans l'exercice de ses fonctions, la CSSF :

a) examine toute demande émanant d'entreprises ou de personnes désireuses de s'établir au Grand-Duché de Luxembourg pour y exercer une ou plusieurs des activités énumérées à l'article 2 et requérant l'agrément du ministre ayant dans ses attributions la CSSF ;

b) établit des statistiques et est autorisée à recueillir à cet effet les données nécessaires auprès de toutes les personnes soumises à sa surveillance ;

c) est autorisée à effectuer le traitement de données à caractère personnel dans le cadre de l'application des compétences légales de la CSSF, et en vue des finalités visées aux articles 2 à 2-3 et dans les lois sectorielles qui y sont référencées et qui déterminent les missions, compétences et pouvoirs de la CSSF ;

d) suit les dossiers et participe aux négociations, sur le plan communautaire et international, relatifs aux problèmes touchant le secteur financier ;

e) présente au Gouvernement toutes suggestions susceptibles d'améliorer l'environnement législatif et réglementaire du secteur financier ;

f) examine toutes autres questions ayant trait à l'activité financière que le ministre ayant dans ses attributions la CSSF lui soumettra.

[…]

Section 7 : Secret

[…] **Art. 16.** …

Art. 16-1. (1) La CSSF est autorisée à collecter et à traiter des données à caractère personnel qui sont nécessaires à l'exercice de ses missions. Ces données à caractère personnel comprennent les données personnelles qui sont indiquées sur les documents officiels ou autres déclarations que les personnes concernées fournissent elles-mêmes ou qui sont transmises par des intermédiaires agissant pour ces personnes, ou qui sont collectées auprès de ces personnes ou auprès de tiers. Les données à caractère personnel collectées et traitées peuvent également concerner des données économiques ou financières des personnes concernées.

(2) La collecte et le traitement des données à caractère personnel visés au paragraphe 1er sont sans préjudice de l'obligation au secret professionnel prévue à l'article 16.

Art. 16-2. Sans préjudice de l'article 6, paragraphe 4, du 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), désigné ci-après « Règlement (UE) 2016/679 », le traitement des données à caractère personnel par la CSSF à une fin autre que celle pour laquelle les données ont été collectées dans le cadre de ses compétences légales est autorisé si :

a) le traitement est effectué dans le cadre d'une procédure ayant pour objet d'imposer une sanction administrative, une mesure de police administrative ou une mesure prudentielle, ou dans le cadre d'actes préparatoires, dans un processus d'audit, de contrôle ou dans le contexte d'une procédure juridictionnelle ;

b) le traitement sert à assurer l'exercice des missions de la CSSF ainsi que le respect des obligations qui en découlent dans le chef de la CSSF, y compris en matière de coopération avec d'autres institutions, autorités, organes ou organismes nationaux, étrangers, européens et internationaux, telle que prévue dans les lois sectorielles régissant lesdites missions ;

c) le traitement est nécessaire pour la poursuite d'une procédure administrative au niveau européen à laquelle la CSSF est partie ;

d) le traitement de données personnelles non pseudonymisées est nécessaire au développement, au contrôle ou à la modification des procédures internes de fonctionnement de la CSSF ; ou

e) le traitement de données personnelles non pseudonymisées est nécessaire pour assurer l'audit de la CSSF, de la direction et des procédures disciplinaires internes de la CSSF.

Art. 16-3. L'obligation de la CSSF de fournir tout ou partie des informations visées à l'article 13, paragraphes 1er, 2 et 3, du Règlement (UE) 2016/679 à la personne concernée lorsque des données personnelles sont collectées auprès d'elle, peut être limitée ou différée par la CSSF dans les cas suivants :

a) lorsque la transmission de ces informations compromet, ou risque de compromettre, l'exercice des missions et compétences prévues aux articles 2 à 2-3 et des pouvoirs légaux de la CSSF, pour autant que l'intérêt poursuivi par la CSSF de ne pas informer la personne concernée prime sur l'intérêt privé de celle-ci.

L'exercice des missions et compétences de la CSSF peut être compromis lorsque la personne concernée fait l'objet d'une procédure administrative ou d'une procédure ayant pour objet d'imposer une sanction administrative, une mesure de police administrative ou une mesure prudentielle, ou lorsque cette personne fait l'objet d'une enquête, ou d'actes préparatoires à ces procédures ou enquêtes, lorsque ces procédures ou enquêtes sont effectuées par la CSSF dans le cadre de l'exécution de ses missions légales, et lorsque l'obligation de la CSSF de respecter pleinement ou immédiatement les droits de la personne concernée ou le plein ou immédiat exercice des droits de la personne concernée porterait atteinte aux besoins ou objectifs de ces procédures ou enquêtes, ou aux actes préparatoires.

Il en est notamment ainsi, si le plein ou immédiat exercice des droits de la personne concernée ou la pleine ou immédiate exécution des obligations de la CSSF est susceptible de mettre la

personne concernée ou des tiers dans une situation permettant d'occulter des faits ou des informations pertinentes dans le cadre desdites procédures ou enquêtes de la CSSF, ou encore d'en tirer un avantage illégitime au détriment de l'exercice des pouvoirs et missions de la CSSF. La CSSF ne peut limiter ou différer son obligation de fournir tout ou partie des informations visées au paragraphe 1er que pendant la durée nécessaire à atteindre la finalité qui justifie la limitation des droits ;

b) si le plein ou immédiat exercice des droits de la personne concernée ou la pleine ou immédiate exécution des obligations de la CSSF menace la stabilité du système bancaire et financier ou des marchés, le maintien de l'ordre public ou la sécurité publique, pour autant que la protection de ces intérêts publics légitimes prévaut sur les intérêts privés de la personne concernée ;

c) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF entrave la défense des intérêts légitimes de la CSSF liés à l'exercice de ses missions légales dans le cadre de procédures juridictionnelles ;

d) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF entrave la poursuite par la CSSF d'une procédure administrative dans laquelle elle est partie, en ce comprise, mais sans s'y limiter, une procédure administrative en non-application ou en violation du droit de l'Union européenne telle que prévue dans le règlement (UE) n°1093/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité bancaire européenne), le règlement (UE) n°1094/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), et le règlement (UE) n°1095/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des marchés financiers) ;

e) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF entrave la communication confidentielle et licite de données en provenance d'autorités ou d'organismes nationaux, étrangers, européens ou internationaux qui transmettent ces données dans l'exercice de leurs compétences respectives, ou qui leur sont transmises par la CSSF dans le cadre de l'exercice de ses compétences légales ;

f) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF porte atteinte à des intérêts légitimes protégés de tiers.

Art. 16-4. L'obligation de la CSSF de fournir tout ou partie des informations visées à l'article 14, paragraphes 1er, 2 et 4, du Règlement (UE) 2016/679 à la personne concernée lorsque des données personnelles sont collectées auprès d'un tiers, peut être limitée ou différée dans les cas visés à l'article 16-3, lettres a) à f), pour autant que l'intérêt public poursuivi par la CSSF de ne pas fournir à la personne concernée ces informations prime sur l'intérêt privé de la personne concernée.

Art. 16-5. Dans les cas visés à l'article 16-3, lettres a) à f), et pour autant que l'intérêt public poursuivi par la CSSF prime sur l'intérêt privé de la personne concernée, la CSSF peut :

a) limiter ou différer la confirmation à la personne concernée que des données à caractère personnel sont traitées, telle que prévue à l'article 15, paragraphe 1er, du Règlement (UE) 2016/679 ;

b) limiter ou différer l'accès, tel que prévu à l'article 15, paragraphe 1er, du Règlement (UE) 2016/679, auxdites données lorsqu'elle procède à un traitement de données à caractère personnel ;

c) limiter ou différer la transmission de tout ou partie des informations visées à l'article 15, paragraphes 1er et 2, du Règlement (UE) 2016/679.

Art. 16-6. La CSSF peut limiter ou différer l'exercice par la personne concernée de son droit à la limitation du traitement de ses données personnelles, tel que prévu à l'article 18 du Règlement (UE) 2016/679, dans les cas visés à l'article 16-3, lettres a) à f), pour autant que l'intérêt public poursuivi par la CSSF de procéder au traitement prime sur l'intérêt privé de la personne concernée.

Art. 16-7. La CSSF peut limiter ou différer le droit de la personne concernée de s'opposer au traitement de ses données à caractère personnel, tel que prévu à l'article 21, paragraphe 1er, du

Règlement (UE) 2016/679, dans les cas visés à l'article 16-3, lettres a) à f), pour autant que l'intérêt public poursuivi par la CSSF de procéder au traitement prime sur l'intérêt privé de la personne concernée.

Art. 16-8. (1) Lorsque la CSSF diffère ou limite, en tout ou en partie, les droits de la personne concernée ou ses propres obligations découlant du Règlement (UE) 2016/679 en application d'une disposition prévue aux articles 16-3 à 16-7, la CSSF lève la limitation à partir du moment où la cause qui la justifie cesse d'exister ou cesse de produire ses effets.

(2) La CSSF informe la personne concernée, par écrit et dans le mois de la survenance de la cause qui justifie la limitation ou le retard, de l'existence de la limitation ou du retard concernant l'exercice par la personne concernée de ses droits ou de ses propres obligations, ainsi que des motifs de la limitation ou retard, à moins que ces informations ne risquent de nuire à la finalité du traitement, de la limitation ou du retard, notamment lorsque ces informations violent le secret professionnel auquel est tenue la CSSF en application de l'article 16, ou lorsque ces informations empêchent la CSSF de poursuivre une procédure administrative ou juridictionnelle à laquelle la CSSF est partie.

(3) La CSSF consigne par écrit les motifs de fait et de droit sur lesquels se fonde sa décision de limiter ou de différer les droits de la personne concernée ou ses propres obligations découlant du Règlement (UE) 2016/679 prise en application d'une disposition prévue aux articles 16-3 à 16-7. Lorsqu'un droit d'une personne concernée ou l'une des obligations incombant à la CSSF est limité ou différé, la CSSF indique la date à partir de laquelle cette limitation deviendra caduque ou, à défaut de date précise, les circonstances permettant d'y mettre fin.

Ces informations sont mises à disposition de la Commission nationale pour la protection des données (ci-après, la « CNPD »), sans préjudice de l'obligation au secret professionnel visée à l'article 16.

(4) La CSSF informe les personnes concernées que leurs données à caractère personnel ont fait l'objet d'un traitement si une procédure administrative ou une enquête a été menée à leur encontre ou si ces personnes ont figuré comme tiers dans une procédure administrative ou une enquête, y compris dans les actes préparatoires, qui a été classée sans qu'une décision n'ait été prise par la CSSF, à moins que ces informations ne violent le secret professionnel visé à l'article 16. L'information leur est fournie sur un support adéquat au plus tard dans les deux mois suivant le classement de la procédure ou de l'enquête.

(5) En cas de limitation des droits de la personne concernée ou de ses propres obligations, la CSSF informe la personne concernée de la possibilité d'introduire une réclamation auprès de la CNPD, conformément à l'article 77 du Règlement (UE) 2016/679, à moins que ces informations ne risquent de nuire à la finalité du ou des traitements et de la limitation, notamment lorsque ces informations violent le secret professionnel auquel est tenue la CSSF en application de l'article 16, ou lorsque ces informations empêchent la CSSF de poursuivre une procédure administrative ou juridictionnelle à laquelle la CSSF est partie.

(6) Sans préjudice du droit de réclamation auprès de la CNPD, la CSSF informe la personne concernée de la possibilité de former un recours juridictionnel, à moins que cette information par la CSSF ne risque de nuire à la finalité du ou des traitements et de la limitation, que cette information viole le secret professionnel auquel est tenue la CSSF en application de l'article 16 ou que cette information empêche la CSSF de poursuivre une procédure administrative ou juridictionnelle à laquelle la CSSF est partie.

(7) La CSSF procède à une vérification régulière de ses systèmes informatiques et procédures internes afin de garantir la conformité du traitement des données à caractère personnel et des limitations aux droits de la personne concernée avec les dispositions du Règlement (UE) 2016/679.

(8) Les données à caractère personnel traitées conformément à la présente loi sont conservées aussi longtemps que nécessaire à l'exercice par la CSSF de ses compétences légales.

Art. 16-9. (1) En cas de limitation des droits de la personne concernée en vertu des articles 16-3 à 16-7, les droits limités ou différés de la personne concernée peuvent être exercés par la CNPD, sans préjudice du secret professionnel de la CSSF prévu à l'article 16.

(2) La CSSF informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la CNPD en application du paragraphe 1er, sauf si cette information nuit à la finalité du ou des traitements et de la limitation ou lorsque cette information viole le secret professionnel de la CSSF prévu à l'article 16 ou empêche la CSSF d'agir ou de se défendre dans une procédure administrative ou juridictionnelle.

(3) Lorsque le droit visé au paragraphe 1er est exercé, la CNPD peut communiquer à la personne concernée le résultat de ses investigations, à moins que cette information ne risque de nuire à la finalité du ou des traitements et de la limitation, que cette information viole le secret professionnel auquel est tenue la CSSF en application de l'article 16 ou que cette information empêche la CSSF de poursuivre une procédure administrative ou juridictionnelle à laquelle la CSSF est partie. Le cas échéant, la CNPD informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. Elle informe également la personne concernée de son droit de former un recours juridictionnel.

*

TEXTE COORDONNE
de la loi modifiée du 7 décembre 2015 sur le secteur des assurances (extraits)

PARTIE 1

La surveillance du secteur des assurances

[…]

Chapitre 2 – *Missions, pouvoirs et responsabilité*

[…]

Art. 5 – ***Données recueillies et statistiques***

Le CAA est autorisé à procéder à l'établissement de statistiques dans le cadre de sa mission auprès de l'ensemble des personnes physiques et morales agréées au Grand-Duché de Luxembourg ou autorisées à y travailler en régime de libre établissement ou de libre prestation de services dans le secteur des assurances.

Les données individuelles ainsi recueillies tombent sous le secret professionnel des organes et des agents du CAA, défini par l'article 7 de la présente loi.

Toutefois le CAA est autorisé à publier les statistiques qu'il établit, à condition que la publication ne contienne pas et ne permette pas de conclure à des données individuelles, à l'exception des statistiques limitativement énumérées par règlement du CAA.

Le CAA est autorisé, en vue des missions visées aux articles 2 et 3 et dans le cadre des pouvoirs énoncés à l'article 4, à effectuer un traitement de données à caractère personnel.

[…]

Chapitre 3 – *Secret professionnel, échange d'informations et promotion de la convergence du contrôle*

[…]

Art. 13-1 – ***Caractéristiques des données à caractère personnel et licéité de leur traitement***

(1) Le CAA est autorisé à collecter et à traiter des données à caractère personnel qui sont nécessaires à l'exercice de ses missions. Ces données à caractère personnel comprennent les données personnelles qui sont indiquées sur les documents officiels ou autres déclarations que les

personnes concernées fournissent elles-mêmes ou qui sont transmises par des intermédiaires agissant pour ces personnes, ou qui sont collectées auprès de ces personnes ou auprès de tiers. Les données à caractère personnel collectées et traitées peuvent également concerner des données économiques ou financières des personnes concernées.

(2) La collecte et le traitement des données à caractère personnel visés au paragraphe 1er sont sans préjudice de l'obligation au secret professionnel prévue à l'article 7.

Art. 13-2 – ***Conditions de changement de la finalité du traitement des données à caractère personnel***

Sans préjudice de l'article 6, paragraphe 4, du Règlement (UE) 2016/679, le traitement des données à caractère personnel par le CAA à une fin autre que celle pour laquelle les données ont été collectées dans le cadre de ses compétences légales est autorisé si :

a) le traitement est effectué dans le cadre d'une procédure ayant pour objet d'imposer une sanction administrative, une mesure de police administrative ou une mesure prudentielle, ou dans le cadre d'actes préparatoires, dans un processus d'audit, de contrôle ou dans le contexte d'une procédure juridictionnelle ;

b) le traitement sert à assurer l'exercice des missions du CAA ainsi que le respect des obligations qui en découlent dans le chef du CAA, y compris en matière de coopération avec d'autres institutions, autorités, organes ou organismes nationaux, étrangers, européens ou internationaux, telle que prévue dans les lois sectorielles régissant lesdites missions ;

c) le traitement est nécessaire pour la poursuite d'une procédure administrative au niveau européen à laquelle le CAA est partie ;

d) le traitement de données personnelles non pseudonymisées est nécessaire au développement, au contrôle ou à la modification des procédures internes de fonctionnement du CAA ;

e) le traitement de données non pseudonymisées est nécessaire pour assurer l'audit du CAA, de la direction et des procédures disciplinaires internes du CAA.

Art. 13-3 – ***Cas de limitation des droits et obligations prévus à l'article 13 du Règlement (UE) 2016/679***

L'obligation du CAA de fournir tout ou partie des informations visées à l'article 13, paragraphes 1er, 2 et 3, du Règlement (UE) 2016/679 à la personne concernée lorsque des données personnelles sont collectées auprès de lui, peut être limitée ou différée par le CAA dans les cas suivants :

a) lorsque la transmission de ces informations compromet, ou risque de compromettre, l'exercice des missions et compétences prévues aux articles 2 et 3 et des pouvoirs légaux du CAA prévus à l'article 4, pour autant que l'intérêt poursuivi par le CAA de ne pas informer la personne concernée prime sur l'intérêt privé de celle-ci.

L'exercice des missions et compétences du CAA peut être compromis lorsque la personne concernée fait l'objet d'une procédure administrative ou d'une procédure ayant pour objet d'imposer une sanction administrative, une mesure de police administrative ou une mesure prudentielle, ou lorsque cette personne fait l'objet d'une enquête, ou d'actes préparatoires à ces procédures ou enquêtes, lorsque ces procédures ou enquêtes sont effectuées par le CAA dans le cadre de l'exécution de ses missions légales, et lorsque l'obligation du CAA de respecter pleinement ou immédiatement les droits de la personne concernée ou le plein ou immédiat exercice des droits de la personne concernée porterait atteinte aux besoins ou objectifs de ces procédures ou enquêtes, ou aux actes préparatoires.

Il en est notamment ainsi, si le plein ou immédiat exercice des droits de la personne concernée ou la pleine ou immédiate exécution des obligations du CAA est susceptible de mettre la personne concernée ou des tiers dans une situation permettant d'occulter des faits ou des informations pertinentes dans le cadre desdites procédures ou enquêtes du CAA, ou encore d'en tirer un avantage illégitime au détriment de l'exercice des pouvoirs et missions de du CAA. Le CAA ne peut limiter ou différer son obligation de fournir tout ou partie des informations visées au paragraphe 1e que pendant la durée nécessaire à atteindre la finalité qui justifie la limitation des droits ;

b) si le plein ou immédiat exercice des droits de la personne concernée ou la pleine ou immédiate exécution des obligations du CAA menace la stabilité financière ou des marchés, le maintien de l'ordre public ou la sécurité publique, pour autant que la protection de ces intérêts publics légitimes prévaut sur les intérêts privés de la personne concernée ;

c) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations du CAA entrave la défense des intérêts légitimes du CAA liés à l'exercice de ses missions légales dans le cadre de procédures juridictionnelles ;

d) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations du CAA entrave la poursuite par le CAA d'une procédure administrative dans laquelle il est partie, en ce comprise, mais sans s'y limiter, une procédure administrative en non-application ou en violation du droit de l'Union européenne telle que prévue dans le règlement (UE) n°1093/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité bancaire européenne), le règlement (UE) n°1094/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), et le règlement (UE) n°1095/2010 du 24 novembre 2010 instituant une autorité européenne de surveillance (Autorité européenne des marchés financiers) ;

e) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations du CAA entrave la communication confidentielle et licite de données en provenance d'autorités ou d'organismes nationaux, étrangers, européens ou internationaux qui transmettent ces données dans l'exercice de leurs compétences respectives, ou qui leur sont transmises par le CAA dans le cadre de l'exercice de ses compétences légales ;

f) si le plein ou immédiat exercice des droits de la personne concernée ou des obligations du CAA porte atteinte à des intérêts légitimes protégés de tiers.

Art. 13-4 – *Cas de limitation des droits et obligations prévus à l'article 14 du Règlement (UE) 2016/679*

L'obligation du CAA de fournir tout ou partie des informations visées à l'article 14, paragraphes 1er, 2 et 4, du Règlement (UE) 2016/679 à la personne concernée lorsque des données personnelles sont collectées auprès d'un tiers, peut être limitée ou différée dans les cas visés à l'article 13-3, lettres a) à f), pour autant que l'intérêt public poursuivi par le CAA de ne pas fournir à la personne concernée ces informations prime sur l'intérêt privé de la personne concernée.

Art. 13-5 – *Cas de limitation des droits et obligations prévus à l'article 15 du Règlement (UE) 2016/679*

Dans les cas visés à l'article 13-3, lettres a) à f), et pour autant que l'intérêt public poursuivi par le CAA prime sur l'intérêt privé de la personne concernée, le CAA peut :

a) limiter ou différer la confirmation à la personne concernée que des données à caractère personnel sont traitées, telle que prévue à l'article 15, paragraphe 1er, du Règlement (UE) 2016/679 ;

b) limiter ou différer l'accès auxdites données lorsqu'il procède à un traitement de données à caractère personnel ;

c) limiter ou différer la transmission de tout ou partie des informations visées à l'article 15, paragraphes 1er et 2, du Règlement (UE) 2016/679.

Art. 13-6 – *Cas de limitation des droits et obligations prévus à l'article 18 du Règlement (UE) 2016/679*

Le CAA peut limiter ou différer l'exercice par la personne concernée de son droit à la limitation du traitement de ses données personnelles, tel que prévu à l'article 18 du Règlement (UE) 2016/679, dans les cas visés à l'article 13-3, lettres a) à f), pour autant que l'intérêt public poursuivi par le CAA de procéder au traitement prime sur l'intérêt privé de la personne concernée.

Art. 13-7 – *Cas de limitation des droits et obligations prévus à l'article 21 du Règlement (UE) 2016/679*

Le CAA peut limiter ou différer le droit de la personne concernée de s'opposer au traitement de ses données à caractère personnel, tel que prévu à l'article 21, paragraphe 1er, du Règlement (UE) 2016/679, dans les cas visés à l'article 13-3, lettres a) à f), pour autant que l'intérêt public

poursuivi par le CAA de procéder au traitement prime sur l'intérêt privé de la personne concernée.

Art. 13-8 – ***Obligations du CAA en cas de limitation des droits et obligations en matière de protection des données confidentielles***

(1) Lorsque le CAA diffère ou limite, en tout ou en partie, les droits de la personne concernée ou ses propres obligations découlant du Règlement (UE) 2016/679 en application d'une disposition prévue aux articles 13-3 à 13-7, le CAA lève la limitation à partir du moment où la cause qui la justifie cesse d'exister ou cesse de produire ses effets.

(2) Le CAA informe la personne concernée, par écrit et dans le mois de la survenance de la cause qui justifie la limitation ou le retard, de l'existence de la limitation ou du retard concernant l'exercice par la personne concernée de ses droits ou de ses propres obligations, ainsi que des motifs de la limitation ou retard, à moins que ces informations ne risquent de nuire à la finalité du traitement, de la limitation ou du retard, notamment lorsque ces informations violent le secret professionnel auquel est tenu le CAA en application de l'article 7, ou lorsque ces informations empêchent le CAA de poursuivre une procédure administrative ou juridictionnelle à laquelle le CAA est partie.

(3) Le CAA consigne par écrit les motifs de fait et de droit sur lesquels se fonde sa décision de limiter ou de différer les droits de la personne concernée ou ses propres obligations découlant du Règlement (UE) 2016/679 prise en application d'une disposition prévue aux articles 13-3 à 13-7. Lorsqu'un droit d'une personne concernée ou l'une des obligations incombant au CAA est limité ou différé, le CAA indique la date à partir de laquelle cette limitation deviendra caduque ou, à défaut de date précise, les circonstances permettant d'y mettre fin.

Ces informations sont mises à disposition de la Commission nationale pour la protection des données (ci-après, la « CNPD »), sans préjudice de l'obligation au secret professionnel visée à l'article 7.

(4) Le CAA informe les personnes concernées que leurs données à caractère personnel ont fait l'objet d'un traitement si une procédure administrative ou une enquête a été menée à leur encontre ou si ces personnes ont figuré comme tiers dans une procédure administrative ou cette enquête, y compris dans les actes préparatoires, qui a été classée sans qu'une décision n'ait été prise par le CAA, à moins que ces informations ne violent le secret professionnel visé à l'article 7. L'information leur est fournie sur un support adéquat au plus tard dans les deux mois suivant le classement de la procédure ou de l'enquête.

(5) En cas de limitation des droits de la personne concernée ou de ses propres obligations, le CAA informe la personne concernée de la possibilité d'introduire une réclamation auprès de la CNPD, conformément à l'article 77 du Règlement (UE) 2016/679, à moins que ces informations ne risquent de nuire à la finalité du ou des traitements et de la limitation, notamment lorsque ces informations violent le secret professionnel auquel est tenu le CAA en application de l'article 7, ou lorsque ces informations empêchent le CAA de poursuivre une procédure administrative ou juridictionnelle à laquelle le CAA est partie.

(6) Sans préjudice du droit de réclamation auprès de la CNPD, le CAA informe la personne concernée de la possibilité de former un recours juridictionnel, à moins que cette information par le CAA ne risque de nuire à la finalité du ou des traitements et de la limitation, que cette information viole le secret professionnel auquel est tenu le CAA en application de l'article 7 ou que cette information empêche le CAA de poursuivre une procédure administrative ou juridictionnelle à laquelle le CAA est partie.

(7) Le CAA procède à une vérification régulière de ses systèmes informatiques et procédures internes afin de garantir la conformité du traitement des données à caractère personnel et des limitations aux droits de la personne concernée avec les dispositions du Règlement (UE) 2016/679.

(8) Les données à caractère personnel traitées conformément à la présente loi sont conservées aussi longtemps que nécessaire à l'exercice par le CAA de ses compétences légales.

Art. 13-9 – ***Exercice des droits par la personne concernée en cas de limitation des droits de la personne concernée***

(1) En cas de limitation des droits de la personne concernée en vertu des articles 13-3 à 13-7, les droits limités ou différés de la personne concernée peuvent être exercés par la CNPD, sans préjudice du secret professionnel du CAA prévu à l'article 7.

(2) Le CAA informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la CNPD en application du paragraphe 1er, sauf si cette information nuit à la finalité du ou des traitements et de la limitation ou lorsque cette information viole le secret professionnel du CAA prévu à l'article 7 ou empêche le CAA d'agir ou de se défendre dans une procédure administrative ou juridictionnelle.

(3) Lorsque le droit visé au paragraphe 1er est exercé, la CNPD peut communiquer à la personne concernée le résultat de ses investigations, à moins que cette information ne risque de nuire à la finalité du ou des traitements et de la limitation, que cette information viole le secret professionnel auquel est tenu le CAA en application de l'article 7 ou que cette information empêche le CAA de poursuivre une procédure administrative ou juridictionnelle dans laquelle le CAA est partie. Le cas échéant, la CNPD informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. Elle informe également la personne concernée de son droit de former un recours juridictionnel.

*

[…]

ANNEXE III

Liste des directives, règlements et décisions émanent de l'Union européenne vises en différents endroits de la loi

[…]

« Règlement (UE) n° 575/2013 » Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012

« Règlement (UE) 2016/679 » : 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 COORDONNE

de la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement (extraits)

[…]

Art. 105. ***Dispositif de financement pour la resolution***

(1) …

(17) Les limitations et garanties prévues aux articles 16-2 à 16-9 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier sont également applicables dans le contexte de l'exécution des missions légales du FRL.

[…]

Art. 154. ***Fonds de garantie des dépôts Luxembourg***

(1) …

(13) Les limitations et garanties prévues aux articles 16-2 à 16-9 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier sont également applicables dans le contexte de l'exécution des missions légales du FGDL.

[…]

*

FICHE FINANCIERE

Le projet de loi du […] concernant la limitation de la portée de certains droits et obligations dans le cadre du règlement général sur la protection des données et portant :

1. exécution, en matière de surveillance du secteur financier et des assurances, du 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) ;
2. modification de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et
3. modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances

n'aura pas d'impact direct sur le budget de l'Etat.

*

FICHE D'EVALUATION D'IMPACT

Coordonnées du projet

Intitulé du projet :	**Projet de loi du […] concernant la limitation de la portée de certains droits et obligations dans le cadre du règlement général sur la protection des données et portant :** **1. exécution, en matière de surveillance du secteur financier et des assurances, du 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) ;** **2. modification de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et** **3. modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances**
Ministère initiateur :	**Ministère des Finances**
Auteur(s) :	**Personnes de contact: Vincent Thurmes et Maureen Wiwinius**
Tél :	**247-82640/247-82669**
Courriel :	**vincent.thurmes@fi.etat.lu/maureen.wiwinius@fi.etat.lu**
Objectif(s) du projet :	**Le projet de loi a pour but d'introduire dans la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier et dans la loi modifiée du 7 décembre 2015 sur le secteur des assurances des limitations facultatives visant b restreindre dans certains cas la pleine application de certaines dispositions du règlement général sur la protection des données afin d'assurer un exercice efficace des missions de la CSSF et du CAA.**

Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s) :
Commission de Surveillance du Secteur Financier et Commissariat aux Assurances
Date : 3.10.2018

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens, …) consultée(s) : Oui ☒ Non ☐
   Si oui, laquelle/lesquelles :
   Commission de Surveillance du Secteur Financier et Commissariat aux Assurances
   Remarques/Observations :

2. Destinataires du projet :
   – Entreprises/Professions libérales : Oui ☒ Non ☐
   – Citoyens : Oui ☒ Non ☐
   – Administrations : Oui ☒ Non ☐

3. Le principe « Think small first » est-il respecté ? Oui ☐ Non ☐ N.a.[1] ☒
   (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)
   Remarques/Observations :

4. Le projet est-il lisible et compréhensible pour le destinataire ? Oui ☒ Non ☐
   Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? Oui ☒ Non ☐
   Remarques/Observations :

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? Oui ☐ Non ☒
   Remarques/Observations :

6. Le projet contient-il une charge administrative[2] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui ☐ Non ☒
   Si oui, quel est le coût administratif[3] approximatif total ? (nombre de destinataires x coût administratif par destinataire)

7. a) Le projet prend-il recours à un échange de données interadministratif (national ou international) plutôt que de demander l'information au destinataire ? Oui ☐ Non ☐ N.a. ☒
   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

1 N.a. : non applicable.

2 Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en oeuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

3 Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple: taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[4] ? Oui ☒ Non ☐ N.a. ☐

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

Il s'agit d'un projet de loi visant à restreindre dans certains cas la pleine application de certaines dispositions du règlement général sur la protection des données dans le cadre des missions de surveillance de la CSSF et du CAA, tout en prévoyant en contrepartie des garanties appropriées afin de respecter les droits fondamentaux des personnes concernées.

8. Le projet prévoit-il :
   - une autorisation tacite en cas de non réponse de l'administration ? Oui ☐ Non ☐ N.a. ☒
   - des délais de réponse à respecter par l'administration ? Oui ☐ Non ☐ N.a. ☒
   - le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? Oui ☐ Non ☐ N.a. ☒

9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? Oui ☐ Non ☐ N.a. ☒

   Si oui, laquelle :

10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? Oui ☐ Non ☐ N.a. ☒

    Sinon, pourquoi ?

11. Le projet contribue-t-il en général à une :

    a) simplification administrative, et/ou à une Oui ☐ Non ☒

    b) amélioration de la qualité réglementaire ? Oui ☒ Non ☐

    Remarques/Observations :

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? Oui ☐ Non ☐ N.a. ☒

13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ? Oui ☐ Non ☒

    Si oui, quel est le délai pour disposer du nouveau système ?

14. Y a-t-il un besoin en formation du personnel de l'administration concernée ? Oui ☐ Non ☐ N.a. ☒

    Si oui, lequel ?

    Remarques/Observations :

---

4 Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

Egalité des chances

15. Le projet est-il :
    – principalement centré sur l'égalité des femmes et des hommes ? Oui ☐ Non ☒
    – positif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒
      Si oui, expliquez de quelle manière :
    – neutre en matière d'égalité des femmes et des hommes ? Oui ☒ Non ☐
      Si oui, expliquez pourquoi :
      II ne fait pas de distinction entre hommes et femmes.
    – négatif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒
      Si oui, expliquez de quelle manière :

16. Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui ☐ Non ☒ N.a. ☐
    Si oui, expliquez de quelle manière :

Directive « services »

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation[5] ? Oui ☐ Non ☐ N.a. ☒
    Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :
    www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[6] ? Oui ☐ Non ☐ N.a. ☒
    Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :
    www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

*

5 Article 15, paragraphe 2 de la directive « services » (cf. Note explicative, p. 10-11)

6 Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p. 10-11)

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)

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,

vu la proposition de la Commission européenne,

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

vu l'avis du Comité économique et social européen ([1]),

vu l'avis du Comité des régions ([2]),

statuant conformément à la procédure législative ordinaire ([3]),

considérant ce qui suit:

(1) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant.

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

(3) La directive 95/46/CE du Parlement européen et du Conseil ([4]) vise à harmoniser la protection des libertés et droits fondamentaux des personnes physiques en ce qui concerne les activités de traitement et à assurer le libre flux des données à caractère personnel entre les États membres.

([1]) JO C 229 du 31.7.2012, p. 90.
([2]) JO C 391 du 18.12.2012, p. 127.
([3]) Position du Parlement européen du 12 mars 2014 (non encore parue au Journal officiel) et position du Conseil en première lecture du 8 avril 2016 (non encore parue au Journal officiel). Position du Parlement européen du 14 avril 2016.
([4]) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

(4) Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique.

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

(6) L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publiquement et à un niveau mondial. Les technologies ont transformé à la fois l'économie et les rapports sociaux, et elles devraient encore faciliter le libre flux des données à caractère personnel au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel.

(7) Ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur. Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant. La sécurité tant juridique que pratique devrait être renforcée pour les personnes physiques, les opérateurs économiques et les autorités publiques.

(8) Lorsque le présent règlement dispose que le droit d'un État membre peut apporter des précisions ou des limitations aux règles qu'il prévoit, les États membres peuvent intégrer des éléments du présent règlement dans leur droit dans la mesure nécessaire pour garantir la cohérence et pour rendre les dispositions nationales compréhensibles pour les personnes auxquelles elles s'appliquent.

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

(10) Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, le niveau de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données devrait être équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union. En ce qui concerne le traitement de données à caractère personnel nécessaire 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, il y a lieu d'autoriser les États membres à maintenir ou à introduire des dispositions nationales destinées à préciser davantage l'application des règles du présent règlement. Parallèlement à la législation générale et horizontale relative à la protection des données mettant en œuvre la directive 95/46/CE, il existe, dans les États membres, plusieurs législations sectorielles spécifiques dans des domaines qui requièrent des dispositions plus précises. Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées «données sensibles»). À cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite.

(11) Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées et les obligations de ceux qui effectuent et déterminent le traitement des données à caractère personnel, ainsi que de prévoir, dans les États membres, des pouvoirs équivalents de surveillance et de contrôle du respect des règles relatives à la protection des données à caractère personnel et des sanctions équivalentes pour les violations.

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

(13) Afin d'assurer un niveau cohérent de protection des personnes physiques dans l'ensemble de l'Union, et d'éviter que des divergences n'entravent la libre circulation des données à caractère personnel au sein du marché intérieur, un règlement est nécessaire pour garantir la sécurité juridique et la transparence aux opérateurs économiques, y compris les micro, petites et moyennes entreprises, pour offrir aux personnes physiques de tous les États membres un même niveau de droits opposables et d'obligations et de responsabilités pour les responsables du traitement et les sous-traitants, et pour assurer une surveillance cohérente du traitement des données à caractère personnel, et des sanctions équivalentes dans tous les États membres, ainsi qu'une coopération efficace entre les autorités de contrôle des différents États membres. Pour que le marché intérieur fonctionne correctement, il est nécessaire que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Pour tenir compte de la situation particulière des micro, petites et moyennes entreprises, le présent règlement comporte une dérogation pour les organisations occupant moins de 250 employés en ce qui concerne la tenue de registres. Les institutions et organes de l'Union, et les États membres et leurs autorités de contrôle sont en outre encouragés à prendre en considération les besoins spécifiques des micro, petites et moyennes entreprises dans le cadre de l'application du présent règlement. Pour définir la notion de micro, petites et moyennes entreprises, il convient de se baser sur l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission ([1]).

(14) La protection conférée par le présent règlement devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel. 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.

(15) 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.

(16) Le présent règlement ne s'applique pas à des questions de protection des libertés et droits fondamentaux ou de libre flux des données à caractère personnel concernant des activités qui ne relèvent pas du champ d'application du droit de l'Union, telles que les activités relatives à la sécurité nationale. Le présent règlement ne s'applique pas au traitement des données à caractère personnel par les États membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union.

(17) Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil ([2]) s'applique au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union. Le règlement (CE) n° 45/2001 et les autres actes juridiques de l'Union applicables audit traitement des données à caractère personnel devraient être adaptés aux principes et aux règles fixés dans le présent règlement et appliqués à la lumière du présent règlement. Pour mettre en place un cadre de protection des données solide et cohérent dans l'Union, il convient, après l'adoption du présent règlement, 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 présent règlement.

(18) Le présent règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une

([1]) Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises [C(2003) 1422] (JO L 124 du 20.5.2003, p. 36).

([2]) 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).

activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.

(19) 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données, fait l'objet d'un acte juridique spécifique de l'Union. Le présent règlement ne devrait dès lors pas s'appliquer aux activités de traitement effectuées à ces fins. Toutefois, les données à caractère personnel traitées par des autorités publiques en vertu du présent règlement devraient, lorsqu'elles sont utilisées à ces fins, être régies par un acte juridique de l'Union plus spécifique, à savoir la directive (UE) 2016/680 du Parlement européen et du Conseil [1]. Les États membres peuvent confier à des autorités compétentes au sens de la directive (UE) 2016/680 des missions qui ne sont pas nécessairement effectuées 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, de manière à ce que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application du droit de l'Union, relève du champ d'application du présent règlement.

En ce qui concerne le traitement de données à caractère personnel par ces autorités compétentes à des fins relevant du champ d'application du présent règlement, les États membres devraient pouvoir maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement. Ces dispositions peuvent déterminer plus précisément les exigences spécifiques au traitement de données à caractère personnel par ces autorités compétentes à ces autres fins, compte tenu de la structure constitutionnelle, organisationnelle et administrative de l'État membre concerné. Lorsque le traitement de données à caractère personnel par des organismes privés relève du champ d'application du présent règlement, celui-ci devrait prévoir la possibilité pour les États membres, sous certaines conditions, de limiter par la loi certaines obligations et certains droits lorsque cette limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir des intérêts spécifiques importants tels que la sécurité publique, ainsi que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Cela est pertinent, par exemple, dans le cadre de la lutte contre le blanchiment d'argent ou des activités des laboratoires de police scientifique.

(20) Bien que le présent règlement s'applique, entre autres, aux activités des juridictions et autres autorités judiciaires, le droit de l'Union ou le droit des États membres pourrait préciser les opérations et procédures de traitement en ce qui concerne le traitement des données à caractère personnel par les juridictions et autres autorités judiciaires. La compétence des autorités de contrôle ne devrait pas s'étendre au traitement de données à caractère personnel effectué par les juridictions dans l'exercice de leur fonction juridictionnelle, afin de préserver l'indépendance du pouvoir judiciaire dans l'accomplissement de ses missions judiciaires, y compris lorsqu'il prend des décisions. Il devrait être possible de confier le contrôle de ces opérations de traitement de données à des organes spécifiques au sein de l'appareil judiciaire de l'État membre, qui devraient notamment garantir le respect des règles du présent règlement, sensibiliser davantage les membres du pouvoir judiciaire aux obligations qui leur incombent en vertu du présent règlement et traiter les réclamations concernant ces opérations de traitement de données.

(21) Le présent règlement s'applique sans préjudice de l'application de la directive 2000/31/CE du Parlement européen et du Conseil [2], et notamment du régime de responsabilité des prestataires de services intermédiaires prévu dans ses articles 12 à 15. Cette directive a pour objectif de contribuer au bon fonctionnement du marché intérieur en assurant la libre circulation des services de la société de l'information entre les États membres.

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

---

[1] 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 (voir page 89 du présent Journal officiel).

[2] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») (JO L 178 du 17.7.2000, p. 1).

(23) Afin de garantir qu'une personne physique ne soit pas exclue de la protection à laquelle elle a droit en vertu du présent règlement, le traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait être soumis au présent règlement lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, qu'un paiement soit exigé ou non. Afin de déterminer si un tel responsable du traitement ou sous-traitant offre des biens ou des services à des personnes concernées qui se trouvent dans l'Union, il y a lieu d'établir s'il est clair que le responsable du traitement ou le sous-traitant envisage d'offrir des services à des personnes concernées dans un ou plusieurs États membres de l'Union. Alors que la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union, peuvent indiquer clairement que le responsable du traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'Union.

(24) Le traitement de données à caractère personnel de personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait également être soumis au présent règlement lorsque ledit traitement est lié au suivi du comportement de ces personnes dans la mesure où il s'agit de leur comportement au sein de l'Union. Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.

(25) Lorsque le droit d'un État membre s'applique en vertu du droit international public, le présent règlement devrait s'appliquer également à un responsable du traitement qui n'est pas établi dans l'Union, par exemple qui se trouve auprès de la représentation diplomatique ou consulaire d'un État membre.

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

(27) Le présent règlement ne s'applique pas aux données à caractère personnel des personnes décédées. Les États membres peuvent prévoir des règles relatives au traitement des données à caractère personnel des personnes décédées.

(28) 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.

(29) Afin d'encourager la pseudonymisation dans le cadre du traitement des données à caractère personnel, des mesures de pseudonymisation devraient être possibles chez un même responsable du traitement, tout en permettant une analyse générale, lorsque celui-ci a pris les mesures techniques et organisationnelles nécessaires afin de garantir, pour le traitement concerné, que le présent règlement est mis en œuvre, et que les informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée précise soient conservées séparément. Le responsable du traitement qui traite les données à caractère personnel devrait indiquer les personnes autorisées à cet effet chez un même responsable du traitement.

(30) 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.

(31) Les autorités publiques auxquelles des données à caractère personnel sont communiquées conformément à une obligation légale pour l'exercice de leurs fonctions officielles, telles que les autorités fiscales et douanières, les cellules d'enquête financière, les autorités administratives indépendantes ou les autorités des marchés financiers responsables de la réglementation et de la surveillance des marchés de valeurs mobilières ne devraient pas être considérées comme des destinataires si elles reçoivent des données à caractère personnel qui sont nécessaires pour mener une enquête particulière dans l'intérêt général, conformément au droit de l'Union ou au droit d'un État membre. Les demandes de communication adressées par les autorités publiques devraient toujours être présentées par écrit, être motivées et revêtir un caractère occasionnel, et elles ne devraient pas porter sur l'intégralité d'un fichier ni conduire à l'interconnexion de fichiers. Le traitement des données à caractère personnel par les autorités publiques en question devrait être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement.

(32) 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 il est accordé.

(33) Souvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Par conséquent, les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet.

(34) Les données génétiques devraient être définies comme les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique, résultant de l'analyse d'un échantillon biologique de la personne physique en question, notamment une analyse des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou de l'analyse d'un autre élément permettant d'obtenir des informations équivalentes.

(35) Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil ([1]) au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro.

(36) L'établissement principal d'un responsable du traitement dans l'Union devrait être le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement des données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union, auquel

([1]) Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).

cas cet autre établissement devrait être considéré comme étant l'établissement principal. L'établissement principal d'un responsable du traitement dans l'Union devrait être déterminé en fonction de critères objectifs et devrait supposer l'exercice effectif et réel d'activités de gestion déterminant les décisions principales quant aux finalités et aux moyens du traitement dans le cadre d'un dispositif stable. Ce critère ne devrait pas dépendre du fait que le traitement ait lieu à cet endroit. La présence et l'utilisation de moyens techniques et de technologies de traitement de données à caractère personnel ou d'activités de traitement ne constituent pas, en elles-mêmes, un établissement principal et ne sont, dès lors, pas des critères déterminants pour un établissement principal. L'établissement principal du sous-traitant devrait être le lieu de son administration centrale dans l'Union ou, s'il ne dispose pas d'une administration centrale dans l'Union, le lieu où se déroule l'essentiel des activités de traitement dans l'Union. Lorsque le responsable du traitement et le sous-traitant sont tous deux concernés, l'autorité de contrôle de l'État membre dans lequel le responsable du traitement a son établissement principal devrait rester l'autorité de contrôle chef de file compétente, mais l'autorité de contrôle du sous-traitant devrait être considérée comme étant une autorité de contrôle concernée et cette autorité de contrôle devrait participer à la procédure de coopération prévue par le présent règlement. En tout état de cause, les autorités de contrôle du ou des États membres dans lesquels le sous-traitant a un ou plusieurs établissements ne devraient pas être considérées comme étant des autorités de contrôle concernées lorsque le projet de décision ne concerne que le responsable du traitement. Lorsque le traitement est effectué par un groupe d'entreprises, l'établissement principal de l'entreprise qui exerce le contrôle devrait être considéré comme étant l'établissement principal du groupe d'entreprises, excepté lorsque les finalités et les moyens du traitement sont déterminés par une autre entreprise.

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

(38) 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 l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. Le consentement du titulaire de la responsabilité parentale ne devrait pas être nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant.

(39) 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 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, règles, garanties et 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 soit limitée au strict minimum. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement 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.

(40) Pour être licite, le traitement de données à caractère personnel devrait être fondé sur le consentement de la personne concernée ou reposer sur tout autre fondement légitime prévu par la loi, soit dans le présent règlement

soit dans une autre disposition du droit national ou du droit de l'Union, ainsi que le prévoit le présent règlement, y compris la nécessité de respecter l'obligation légale à laquelle le responsable du traitement est soumis 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.

(41) Lorsque le présent règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné. Cependant, cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée «Cour de justice») et de la Cour européenne des droits de l'homme.

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

(43) Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution.

(44) Le traitement devrait être considéré comme licite lorsqu'il est nécessaire dans le cadre d'un contrat ou de l'intention de conclure un contrat.

(45) Lorsque le traitement est effectué conformément à une obligation légale à laquelle le responsable du traitement est soumis ou lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, le traitement devrait avoir un fondement dans le droit de l'Union ou dans le droit d'un État membre. Le présent règlement ne requiert pas de disposition légale spécifique pour chaque traitement individuel. Une disposition légale peut suffire pour fonder plusieurs opérations de traitement basées sur une obligation légale à laquelle le responsable du traitement est soumis ou lorsque le traitement est nécessaire pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique. Il devrait également appartenir au droit de l'Union ou au droit d'un État membre de déterminer la finalité du traitement. Par ailleurs, ce droit pourrait préciser les conditions générales du présent règlement régissant la licéité du traitement des données à caractère personnel, établir les spécifications visant à déterminer le responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal. Il devrait, également, appartenir au droit de l'Union ou au droit d'un État membre de déterminer si le responsable du traitement exécutant une mission d'intérêt public ou relevant de l'exercice de l'autorité publique devrait être une autorité publique ou une autre personne physique ou morale de droit public ou, lorsque l'intérêt public le commande, y compris à des fins de santé, telles que la santé publique, la protection sociale et la gestion des services de soins de santé, de droit privé, telle qu'une association professionnelle.

(46) Le traitement de données à caractère personnel devrait être également considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne

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

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.

(47) Les intérêts légitimes d'un responsable du traitement, y compris ceux d'un responsable du traitement à qui les données à caractère personnel peuvent être communiquées, ou d'un tiers peuvent constituer une base juridique pour le traitement, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent, compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. Un tel intérêt légitime pourrait, par exemple, exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans des situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service. En tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée. Les intérêts et droits fondamentaux de la personne concernée pourraient, en particulier, prévaloir sur l'intérêt du responsable du traitement lorsque des données à caractère personnel sont traitées dans des circonstances où les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur. Étant donné qu'il appartient au législateur de prévoir par la loi la base juridique pour le traitement des données à caractère personnel par les autorités publiques, cette base juridique ne devrait pas s'appliquer aux traitements effectués par des autorités publiques dans l'accomplissement de leurs missions. Le traitement de données à caractère personnel strictement nécessaire à des fins de prévention de la fraude constitue également un intérêt légitime du responsable du traitement concerné. Le traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime.

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

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

(50) 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 ou le droit d'un État membre 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 ou le droit d'un État membre 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.

Lorsque la personne concernée a donné son consentement ou que le traitement est fondé sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir, en particulier, d'importants objectifs d'intérêt public général, le responsable du traitement devrait être autorisé à effectuer un traitement ultérieur des données à caractère personnel indépendamment de la compatibilité des finalités. En tout état de cause, l'application des principes énoncés dans le présent règlement et, en particulier, l'information de la personne concernée au sujet de ces autres finalités et de ses droits, y compris le droit de s'opposer au traitement, devraient être assurées. Le fait, pour le responsable du traitement, de révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre à une autorité compétente les données à caractère personnel concernées dans des cas individuels ou dans plusieurs cas relatifs à une même infraction pénale ou à des mêmes menaces pour la sécurité publique devrait être considéré comme relevant de l'intérêt légitime du responsable du traitement. Néanmoins, cette transmission dans l'intérêt légitime du responsable du traitement ou le traitement ultérieur des données à caractère personnel devrait être interdit lorsque le traitement est incompatible avec une obligation de confidentialité légale, professionnelle ou toute autre obligation de confidentialité contraignante.

(51) 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 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. De telles données à caractère personnel ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne soit autorisé dans des cas spécifiques prévus par le présent règlement, compte tenu du fait que le droit d'un État membre peut prévoir des dispositions spécifiques relatives à la protection des données visant à adapter l'application des règles du présent règlement en vue de respecter une obligation légale ou pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Outre les exigences spécifiques applicables à ce traitement, 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.

(52) Des dérogations à l'interdiction de traiter des catégories particulières de données à caractère personnel devraient également être autorisées lorsque le droit de l'Union ou le droit d'un État membre le prévoit, et sous réserve de garanties appropriées, de manière à protéger les données à caractère personnel et d'autres droits fondamentaux, lorsque l'intérêt public le commande, notamment le traitement des données à caractère personnel dans le domaine du droit du travail et du droit de la protection sociale, y compris les retraites, et à des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé. Ces dérogations sont possibles à des fins de santé, en ce compris la santé publique et la gestion des services de soins de santé, en particulier pour assurer la qualité et l'efficience des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie, ou à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Une dérogation devrait, en outre, permettre le traitement de ces données à caractère personnel, si cela est nécessaire aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice, que ce soit dans le cadre d'une procédure judiciaire, administrative ou extrajudiciaire.

(53) Les catégories particulières de données à caractère personnel qui méritent une protection plus élevée ne devraient être traitées qu'à des fins liées à la santé, lorsque cela est nécessaire pour atteindre ces finalités dans l'intérêt des personnes physiques et de la société dans son ensemble, notamment dans le cadre de la gestion des services et des systèmes de soins de santé ou de protection sociale, y compris le traitement, par les autorités de gestion et les autorités centrales de santé nationales, de ces données, en vue du contrôle de la qualité, de l'information des gestionnaires et de la supervision générale, au niveau national et local, du système de soins de santé ou de protection sociale et en vue d'assurer la continuité des soins de santé ou de la protection sociale et des soins de santé transfrontaliers ou à des fins de sécurité, de surveillance et d'alerte sanitaires, ou à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, sur la base du droit de l'Union ou du droit des États membres qui doit répondre à un objectif d'intérêt public, ainsi que pour des

études menées dans l'intérêt public dans le domaine de la santé publique. Le présent règlement devrait dès lors prévoir des conditions harmonisées pour le traitement des catégories particulières de données à caractère personnel relatives à la santé, pour répondre à des besoins spécifiques, en particulier lorsque le traitement de ces données est effectué pour certaines fins liées à la santé par des personnes soumises à une obligation légale de secret professionnel. Le droit de l'Union ou le droit des États membres devrait prévoir des mesures spécifiques et appropriées de façon à protéger les droits fondamentaux et les données à caractère personnel des personnes physiques. Les États membres devraient être autorisés à maintenir ou à introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé. Toutefois, cela ne devrait pas entraver le libre flux des données à caractère personnel au sein de l'Union lorsque ces conditions s'appliquent au traitement transfrontalier de ces données.

(54) 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) nº 1338/2008 du Parlement européen et du Conseil ([1]), à savoir tous les éléments relatifs à la santé, à savoir 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, tels que les employeurs ou les compagnies d'assurance et les banques.

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

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

(57) 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.

(58) Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels. Ces informations pourraient être fournies sous forme électronique, par exemple via un site internet lorsqu'elles s'adressent au public. Ceci vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne. Les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre.

(59) 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.

([1]) Règlement (CE) nº 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).

(60) 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 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.

(61) 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.

(62) Toutefois, il n'est pas nécessaire d'imposer l'obligation de fournir des informations lorsque la personne concernée dispose déjà de ces informations, lorsque l'enregistrement ou la communication des données à caractère personnel est expressément prévu par la loi ou lorsque la communication d'informations à la personne concernée se révèle impossible ou exigerait des efforts disproportionnés. Tel pourrait être le cas, notamment, lorsqu'il s'agit d'un traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. À cet égard, devraient être pris en considération le nombre de personnes concernées, l'ancienneté des données, ainsi que les garanties appropriées éventuelles adoptées.

(63) 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 ou intervention administrés. 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. Lorsque c'est possible, le responsable du traitement devrait pouvoir donner l'accès à distance à un système sécurisé permettant à la personne concernée d'accéder directement aux données à caractère personnel la concernant. 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.

(64) Le responsable du traitement devrait prendre toutes les mesures raisonnables pour vérifier l'identité d'une personne concernée qui demande l'accès à des données, en particulier dans le cadre des services et identifiants en ligne. Un responsable du traitement ne devrait pas conserver des données à caractère personnel à la seule fin d'être en mesure de réagir à d'éventuelles demandes.

(65) 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 ou du droit d'un État membre auquel le responsable du traitement est soumis. En particulier, les personnes concernées devraient avoir le droit d'obtenir que leurs données à caractère personnel soient effacées et ne soient plus traitées, lorsque ces données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de

données à caractère personnel les concernant, ou encore lorsque le traitement de leurs données à caractère personnel ne respecte pas d'une autre manière le présent règlement. Ce droit est pertinent, en particulier, lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'internet. La personne concernée devrait pouvoir exercer ce droit nonobstant le fait qu'elle n'est plus un enfant. Toutefois, la conservation ultérieure des données à caractère personnel devrait être licite lorsqu'elle est nécessaire à l'exercice du droit à la liberté d'expression et d'information, au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ou à la constatation, à l'exercice ou à la défense de droits en justice.

(66) 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.

(67) 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.

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

(69) Lorsque des données à caractère personnel pourraient être traitées de manière licite parce que le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, ou en raison des intérêts légitimes du responsable du traitement ou d'un tiers, les personnes concernées devraient néanmoins avoir le droit de s'opposer au traitement de toute donnée à caractère personnel en rapport avec leur 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.

(70) Lorsque des données à caractère personnel sont traitées à des fins de prospection, la personne concernée devrait avoir le droit, à tout moment et sans frais, de s'opposer à ce traitement, y compris le profilage dans la mesure où il est lié à une telle prospection, qu'il s'agisse d'un traitement initial ou ultérieur. Ce droit devrait être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information.

(71) 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 le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine. Ce type de traitement inclut le «profilage» qui consiste en toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements, dès lors qu'il produit des effets juridiques concernant la personne en question ou qu'il l'affecte de façon similaire de manière significative. Toutefois, la prise de décision fondée sur un tel traitement, y compris le profilage, devrait être permise lorsqu'elle est expressément autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis, y compris aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale conformément aux règles, normes et recommandations des institutions de l'Union ou des organes de contrôle nationaux, et d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement, ou nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, ou si la personne concernée a donné son consentement explicite. 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 que dans des conditions spécifiques.

(72) Le profilage est soumis aux règles du présent règlement régissant le traitement des données à caractère personnel, par exemple le fondement juridique du traitement ou les principes en matière de protection des données. Le comité européen de la protection des données établi par le présent règlement (ci-après dénommé «comité») devrait pouvoir publier des directives à cet égard.

(73) 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 d'opposition, aux décisions fondées sur le profilage, 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 le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité publique, y compris la protection de la vie humaine, particulièrement en réponse à des catastrophes d'origine naturelle ou humaine, 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 ou de manquements à la déontologie des professions réglementées, et pour garantir 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, le traitement ultérieur de données à caractère personnel archivées pour fournir des informations spécifiques relatives au comportement politique dans le cadre des régimes des anciens États totalitaires 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. Il y a lieu que ces limitations respectent les exigences énoncées par la Charte et par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

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

(75) Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier: lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.

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

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

(78) 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. Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. 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.

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

(80) Lorsqu'un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union traite des données à caractère personnel de personnes concernées qui se trouvent dans l'Union et que ses activités de traitement sont liées à l'offre de biens ou de services à ces personnes dans l'Union, qu'un paiement leur soit demandé ou non, ou au suivi de leur comportement, dans la mesure où celui-ci a lieu au sein de l'Union, il convient que le responsable du traitement ou le sous-traitant désigne un représentant, à moins que le traitement soit occasionnel, n'implique pas un traitement, à grande échelle, de catégories particulières de données à caractère personnel ou le traitement de données à caractère personnel relatives à des condamnations pénales et à des infractions, et soit peu

susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement, ou si le responsable du traitement est une autorité publique ou un organisme public. Le représentant devrait agir pour le compte du responsable du traitement ou du sous-traitant et peut être contacté par toute autorité de contrôle. Le représentant devrait être expressément désigné par un mandat écrit du responsable du traitement ou du sous-traitant pour agir en son nom en ce qui concerne les obligations qui lui incombent en vertu du présent règlement. La désignation de ce représentant ne porte pas atteinte aux responsabilités du responsable du traitement ou du sous-traitant au titre du présent règlement. Ce représentant devrait accomplir ses tâches conformément au mandat reçu du responsable du traitement ou du sous-traitant, y compris coopérer avec les autorités de contrôle compétentes en ce qui concerne toute action entreprise pour assurer le respect du présent règlement. Le représentant désigné devrait faire l'objet de procédures coercitives en cas de non-respect du présent règlement par le responsable du traitement ou le sous-traitant.

(81) Afin que les exigences du présent règlement soient respectées dans le cadre d'un traitement réalisé par un sous-traitant pour le compte du responsable du traitement, lorsque ce dernier confie des activités de traitement à un sous-traitant, le responsable du traitement ne devrait faire appel qu'à des sous-traitants présentant des garanties suffisantes, notamment en termes de connaissances spécialisées, de fiabilité et de ressources, pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont aux exigences du présent règlement, y compris en matière de sécurité du traitement. L'application par un sous-traitant 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 au titre du droit de l'Union ou du droit d'un État membre, liant le sous-traitant au responsable du traitement, définissant l'objet et la durée du traitement, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées, 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 peuvent choisir de recourir à un contrat particulier ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par une autorité de contrôle conformément au mécanisme de contrôle de la cohérence, puis par la Commission. 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 des données à caractère personnel.

(82) Afin de démontrer qu'il respecte le présent règlement, le responsable du traitement ou le sous-traitant devrait tenir des registres pour les activités de traitement relevant de sa responsabilité. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à la disposition de celle-ci, sur demande, pour qu'ils servent au contrôle des opérations de traitement.

(83) 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 ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral.

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

(85) Une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel

protégées par le secret professionnel ou tout autre dommage économique ou social important. En conséquence, dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il convient qu'il le notifie à l'autorité de contrôle 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, la notification devrait être assortie des motifs du retard et des informations peuvent être fournies de manière échelonnée sans autre retard indu.

(86) Le responsable du traitement devrait communiquer une violation de données à caractère personnel à la personne concernée dans les meilleurs délais lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique afin qu'elle puisse prendre les précautions qui s'imposent. La communication devrait décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels. Il convient que de telles communications aux personnes concernées soient effectuées aussi rapidement qu'il est raisonnablement possible et en coopération étroite avec l'autorité de contrôle, dans le respect des directives données par celle-ci ou par d'autres autorités compétentes, telles que les autorités répressives. Par exemple, la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données à caractère personnel ou la survenance de violations similaires peut justifier un délai plus long pour la communication.

(87) Il convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs fixés par le présent règlement.

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

(89) La directive 95/46/CE prévoyait une obligation générale de notifier les traitements de données à caractère personnel aux autorités de contrôle. Or, cette obligation génère une charge administrative et financière, sans pour autant avoir 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 portée, de leur contexte et de leurs finalités. Ces types d'opérations de traitement peuvent 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.

(90) 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 la portée, 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.

(91) Cela devrait s'appliquer en particulier aux opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé, par exemple, en raison de leur caractère sensible, lorsque, en conformité avec l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle, ainsi qu'à d'autres opérations de traitement qui engendrent un risque élevé pour les droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations,

il est plus difficile pour ces personnes d'exercer leurs droits. Une analyse d'impact relative à la protection des données devrait également être effectuée lorsque des données à caractère personnel sont traitées en vue de prendre des décisions relatives à des personnes physiques spécifiques à la suite d'une évaluation systématique et approfondie d'aspects personnels propres à des personnes physiques sur la base du profilage desdites données ou à la suite du traitement de catégories particulières de données à caractère personnel, de données biométriques ou de données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes. Une analyse d'impact relative à la protection des données est de même requise aux fins de la surveillance à grande échelle de zones accessibles au public, en particulier lorsque des dispositifs opto-électroniques sont utilisés, ou pour toute autre opération pour laquelle l'autorité de contrôle compétente considère que le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, en particulier parce qu'elles empêchent ces personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat, ou parce qu'elles sont effectuées systématiquement à grande échelle. Le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. Dans de tels cas, une analyse d'impact relative à la protection des données ne devrait pas être obligatoire.

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

(93) Au moment de l'adoption du droit d'un État membre qui fonde l'exercice des missions de l'autorité publique ou de l'organisme public concernés et qui règlemente l'opération ou l'ensemble d'opérations de traitement spécifiques, les États membres peuvent estimer qu'une telle analyse est nécessaire préalablement aux activités de traitement.

(94) Lorsqu'il ressort d'une analyse d'impact relative à la protection des données que, en l'absence des garanties, de mesures de sécurité et de mécanismes pour atténuer le risque, le traitement engendrerait un risque élevé pour les droits et libertés des personnes physiques et que le responsable du traitement est d'avis que le risque ne peut être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts de mise en œuvre, il y a lieu de consulter l'autorité de contrôle avant le début des opérations de traitement. Certains types de traitements et l'ampleur et la fréquence des traitements sont susceptibles d'engendrer un tel risque élevé et peuvent également causer un dommage ou porter atteinte aux droits et libertés d'une personne physique. L'autorité de contrôle devrait répondre à la demande de consultation dans un délai déterminé. Toutefois, l'absence de réaction de l'autorité de contrôle dans le délai imparti devrait être sans préjudice de toute intervention de sa part 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, les résultats d'une analyse d'impact relative à la protection des données réalisée en ce qui concerne le traitement en question peuvent être soumis à l'autorité de contrôle, notamment les mesures envisagées pour atténuer le risque pour les droits et libertés des personnes physiques.

(95) Le sous-traitant devrait aider le responsable du traitement, si nécessaire et sur demande, à assurer le respect des obligations découlant de la réalisation des analyses d'impact relatives à la protection des données et de la consultation préalable de l'autorité de contrôle.

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

(97) Lorsque le traitement est réalisé par une autorité publique, à l'exception des juridictions ou des autorités judiciaires indépendantes agissant dans l'exercice de leur fonction juridictionnelle, lorsque, dans le secteur privé, il est effectué par un responsable du traitement dont les activités de base consistent en opérations de traitement exigeant un suivi régulier et systématique à grande échelle des personnes concernées, ou lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données à caractère personnel et de données relatives à des condamnations pénales et à des infractions, une personne possédant des connaissances spécialisées de la législation et des pratiques en matière de protection des données devrait aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement. Dans le secteur privé, les activités de base d'un responsable du traitement ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaire. Le niveau de connaissances spécialisées requis devrait être déterminé 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. De tels délégués à la protection des données, qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance.

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

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

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

(101) Les flux de données à caractère personnel à destination et en provenance de pays en dehors de l'Union et d'organisations internationales sont nécessaires au développement du commerce international et de la coopération internationale. L'augmentation de ces flux a créé de nouveaux enjeux et de nouvelles préoccupations en ce qui concerne la protection des données à caractère personnel. Cependant, il importe que, lorsque des données à caractère personnel sont transférées 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 soit pas 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 à 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 dispositions du présent règlement relatives au transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales sont respectées par le responsable du traitement ou le sous-traitant.

(102) Le présent règlement s'entend sans préjudice des accords internationaux conclus entre l'Union et les pays tiers en vue de réglementer le transfert des données à caractère personnel, y compris les garanties appropriées au bénéfice des personnes concernées. Les États membres peuvent conclure des accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales dans la mesure où ces accords n'affectent pas le présent règlement ou toute autre disposition du droit de l'Union et prévoient un niveau approprié de protection des droits fondamentaux des personnes concernées.

(103) La Commission peut décider, avec effet dans l'ensemble de l'Union, qu'un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale offre un niveau adéquat de protection des données, assurant ainsi une sécurité juridique et une uniformité dans l'ensemble l'Union en ce qui concerne le pays tiers ou l'organisation internationale qui est réputé offrir un tel niveau de protection. Dans ce cas, les transferts de données à caractère personnel vers ce pays tiers ou cette organisation internationale peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autre autorisation. La Commission peut également décider, après en avoir informé le pays tiers ou l'organisation internationale et lui avoir fourni une justification complète, de révoquer une telle décision.

(104) Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait, dans son évaluation d'un pays tiers, d'un territoire ou d'un secteur déterminé dans un pays tiers, prendre en considération la manière dont un pays tiers déterminé respecte l'état de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, y compris la législation sur la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal. Lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision d'adéquation, il y a lieu de tenir compte de critères clairs et objectifs, telles que les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union, en particulier

quand les données à caractère personnel sont traitées dans un ou plusieurs secteurs spécifiques. Plus particulièrement, le pays tiers devrait assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités de protection des données des États membres, et les personnes concernées devraient se voir octroyer des droits effectifs et opposables ainsi que des possibilités effectives de recours administratif et juridictionnel.

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

(106) La Commission devrait surveiller le fonctionnement des décisions relatives au niveau de protection offert par un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou par une organisation internationale, et surveiller le fonctionnement des décisions adoptées sur la base de l'article 25, paragraphe 6, ou de l'article 26, paragraphe 4, de la directive 95/46/CE. Dans ses décisions d'adéquation, la Commission devrait prévoir un mécanisme d'examen périodique de leur fonctionnement. Cet examen périodique devrait être effectué en consultation avec le pays tiers ou l'organisation internationale en question et tenir compte de l'ensemble des évolutions présentant un intérêt dans le pays tiers ou au sein de l'organisation internationale. Aux fins de la surveillance et de la réalisation des examens périodiques, la Commission devrait prendre en considération les observations et les conclusions du Parlement européen et du Conseil, ainsi que d'autres organes et sources pertinents. La Commission devrait évaluer le fonctionnement desdites décisions dans un délai raisonnable et communiquer toute conclusion pertinente au comité au sens du règlement (UE) nº 182/2011 du Parlement européen et du Conseil [1] établi en vertu du présent règlement, au Parlement européen et au Conseil.

(107) La Commission peut constater qu'un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale n'assure plus un niveau adéquat de protection des données. En conséquence, le transfert de données à caractère personnel vers ce pays tiers ou à cette organisation internationale devrait être interdit, à moins que les exigences du présent règlement relatives aux transferts faisant l'objet de garanties appropriées, y compris des règles d'entreprise contraignantes et des dérogations pour des situations particulières, soient respectées. Dans ce cas, il y aurait lieu de prévoir des consultations entre la Commission et le pays tiers ou l'organisation internationale en question. La Commission devrait informer en temps utile le pays tiers ou l'organisation internationale des motifs de sa conclusion et engager des consultations avec ceux-ci en vue de remédier à la situation.

(108) En l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant devrait prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. Ces garanties peuvent consister à recourir à des règles d'entreprise contraignantes, des clauses types de protection des données adoptées par la Commission, des clauses types de protection des données adoptées par une autorité de contrôle ou des clauses contractuelles autorisées par une autorité de contrôle. Ces garanties devraient assurer le respect des exigences en matière de protection des données et des droits des personnes concernées d'une manière appropriée au 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 de protection des données par défaut. Des transferts peuvent également être effectués par des autorités publiques ou des organismes publics avec des autorités publiques ou des organismes publics dans des pays tiers ou avec des organisations internationales exerçant des missions ou fonctions correspondantes, y compris sur la base de dispositions à intégrer dans des arrangements administratifs, telles qu'un protocole d'accord, prévoyant des droits opposables et effectifs pour les personnes concernées. L'autorisation de l'autorité de contrôle compétente devrait être obtenue lorsque ces garanties sont prévues dans des arrangements administratifs qui ne sont pas juridiquement contraignants.

(109) La possibilité qu'ont les responsables du traitement et les sous-traitants de recourir à des clauses types de protection des données adoptées par la Commission ou par une autorité de contrôle ne devrait pas les empêcher

[1] Règlement (UE) nº 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).

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 une autorité de contrôle et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées. Les responsables du traitement et les sous-traitants devraient être encouragés à fournir des garanties supplémentaires par l'intermédiaire d'engagements contractuels qui viendraient compléter les clauses types de protection.

(110) Un groupe d'entreprises ou un groupe d'entreprises engagées dans une activité économique conjointe devrait pouvoir recourir à des règles d'entreprise contraignantes approuvées pour ses transferts internationaux de l'Union vers des entités du même groupe d'entreprises, ou du même groupe d'entreprises engagées dans une activité économique conjointe, à condition que ces règles d'entreprise incluent tous les principes essentiels et les droits opposables pour assurer des garanties appropriées pour les transferts ou catégories de transferts de données à caractère personnel.

(111) Il y a lieu de prévoir 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 ou le droit d'un État membre 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 et, lorsque celui-ci 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.

(112) 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 autorités de la concurrence, administrations fiscales ou douanières, entre autorités de surveillance financière, entre services chargés des questions de sécurité sociale ou relatives à la santé publique, par exemple aux fins de la recherche des 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 d'une décision d'adéquation, le droit de l'Union ou le droit d'un État membre peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories particulières de données vers un pays tiers ou à une organisation internationale. Les États membres devraient notifier ces dispositions à la Commission. Tout transfert vers une organisation humanitaire internationale 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.

(113) Les transferts qui peuvent être qualifiés de non répétitifs et qui ne touchent qu'un nombre limité de personnes concernées pourraient également être autorisés aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement, lorsque ces intérêts prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée et lorsque le responsable du traitement a évalué toutes les circonstances entourant le transfert de données. Le responsable du traitement devrait accorder une attention particulière à la nature des données à caractère personnel, à la finalité et à la durée de la ou des opérations de traitement envisagées ainsi qu'à la situation dans le pays d'origine, le pays tiers et le pays de destination finale, et devrait prévoir des garanties appropriées pour protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement de leurs données à caractère personnel. De tels transferts ne devraient être possibles que dans les cas résiduels dans lesquels aucun des autres motifs de transfert ne sont applicables. À des fins de recherche scientifique ou historique ou à des fins statistiques, il y a lieu de prendre en considération les attentes légitimes de la société en matière de progrès des connaissances. Le responsable du traitement devrait informer l'autorité de contrôle et la personne concernée du transfert.

(114) 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.

(115) Certains pays tiers adoptent des lois, des règlements et d'autres actes juridiques qui visent à réglementer directement les activités de traitement effectuées par des personnes physiques et morales qui relèvent de la compétence des États membres. 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, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre. 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 ou le d'un État membre auquel le responsable du traitement est soumis.

(116) 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 peuvent être confrontées à l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités exercées en dehors de leurs frontières. Leurs efforts pour collaborer dans le contexte transfrontalier peuvent également être freinés par les pouvoirs insuffisants dont elles disposent en matière de prévention ou de recours, par l'hétérogénéité des régimes juridiques et par des obstacles pratiques tels que le manque de ressources. En conséquence, il est nécessaire de favoriser une coopération plus étroite entre les autorités de contrôle de la protection des données, pour les aider à échanger des informations et mener des enquêtes avec leurs homologues internationaux. Aux fins d'élaborer des mécanismes de coopération internationale destinés à faciliter et à mettre en place une assistance mutuelle internationale pour faire appliquer la législation relative à la protection des données à caractère personnel, la Commission et les autorités de contrôle devraient échanger des informations et coopérer dans le cadre d'activités liées à l'exercice de leurs compétences avec les autorités compétentes dans les pays tiers, sur une base réciproque et conformément au présent règlement.

(117) La mise en place d'autorités de contrôle dans les États membres, habilitées à exercer leurs missions et leurs pouvoirs en toute indépendance, est un élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Les États membres devraient pouvoir mettre en place plusieurs autorités de contrôle en fonction de leur structure constitutionnelle, organisationnelle et administrative.

(118) L'indépendance des autorités de contrôle ne devrait pas signifier que celles-ci ne peuvent être soumises à des mécanismes de contrôle ou de suivi de leur gestion financière ni à un contrôle juridictionnel.

(119) Lorsqu'un État membre met en place plusieurs autorités de contrôle, il devrait établir par la loi des dispositifs garantissant la participation effective de ces autorités au mécanisme de contrôle de la cohérence. Il devrait en particulier désigner l'autorité de contrôle qui sert de point de contact unique, permettant une participation efficace de ces autorités au mécanisme, afin d'assurer une coopération rapide et aisée avec les autres autorités de contrôle, le comité et la Commission.

(120) Il convient que chaque autorité de contrôle soit dotée des moyens financiers et humains, ainsi que des locaux et des infrastructures nécessaires à la bonne exécution de ses missions, y compris celles qui sont liées à l'assistance mutuelle et à la coopération avec d'autres autorités de contrôle dans l'ensemble de l'Union. Chaque autorité de contrôle devrait disposer d'un budget annuel public propre, qui peut faire partie du budget global national ou d'une entité fédérée.

(121) Les conditions générales applicables au(x) membre(s) de l'autorité de contrôle devraient être fixées par la loi dans chaque État membre et devraient prévoir notamment que ces membres sont nommés, selon une procédure transparente, par le parlement, le gouvernement ou le chef d'État de cet État membre, sur proposition du gouvernement ou d'un membre du gouvernement, ou du parlement ou d'une chambre du parlement, ou par un organisme indépendant qui en a été chargé en vertu du droit d'un État membre,. Afin de garantir l'indépendance de l'autorité de contrôle, il convient que le membre ou les membres de celle-ci agissent avec intégrité, s'abstiennent de tout acte incompatible avec leurs fonctions et n'exercent, pendant la durée de leur mandat, aucune activité professionnelle incompatible, rémunérée ou non. Chaque autorité de contrôle devrait disposer de ses propres agents, choisis par elle-même ou un organisme indépendant établi par le droit d'un État membre, qui devraient être placés sous les ordres exclusifs du membre ou des membres de l'autorité de contrôle.

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

couvrir, notamment, le traitement dans le cadre d'activités menées par un établissement du responsable du traitement ou du sous-traitant sur le territoire de l'État membre dont elle relève, le traitement de données à caractère personnel effectué par des autorités publiques ou des organismes privés agissant dans l'intérêt public, le traitement affectant des personnes concernées sur le territoire de l'État membre dont elle relève, ou encore le traitement effectué par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union lorsque ce traitement vise des personnes concernées résidant sur le territoire de l'État membre dont elle relève. Cela devrait comprendre notamment le traitement des réclamations introduites par les personnes concernées, la conduite d'enquêtes sur l'application du présent règlement et la sensibilisation du public aux risques, règles, garanties et droits liés au traitement des données à caractère personnel.

(123) Il y a lieu que les autorités de contrôle surveillent l'application des dispositions en vertu du présent règlement 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 le libre flux de ces données dans le marché intérieur. À cet effet, les autorités de contrôle devraient coopérer entre elles et avec la Commission sans qu'un accord doive être conclu entre les États membres sur la fourniture d'une assistance mutuelle ou sur une telle coopération.

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

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

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

(127) Chaque autorité de contrôle qui ne fait pas office d'autorité de contrôle chef de file devrait être compétente pour traiter les cas de portée locale lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres mais que l'objet du traitement spécifique ne se rapporte qu'à un traitement effectué dans un seul État membre et ne porte que sur des personnes concernées de ce seul État membre, par exemple lorsqu'il s'agit de traiter des données à caractère personnel relatives à des employés dans le contexte des relations de travail propre à un État membre. Dans ces cas, l'autorité de contrôle devrait informer sans tarder l'autorité de contrôle chef de file de la question. Après avoir été informée, l'autorité de contrôle chef de file devrait décider si elle traitera le cas en vertu de la disposition relative à la coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées (ci-après dénommé «mécanisme de guichet unique»), ou si l'autorité de contrôle qui l'a informée devrait traiter le cas au niveau local. Lorsqu'elle décide si elle traitera le cas, l'autorité de contrôle chef de file devrait considérer s'il existe un établissement du responsable du traitement ou du sous-traitant dans l'État membre dont relève l'autorité de contrôle qui l'a informée, afin d'assurer l'exécution effective d'une décision à l'égard du responsable du traitement ou du sous-traitant. Lorsque l'autorité de contrôle chef de file décide de

traiter le cas, l'autorité de contrôle qui l'a informée devrait avoir la possibilité de soumettre un projet de décision, dont l'autorité de contrôle chef de file devrait tenir le plus grand compte lorsqu'elle élabore son projet de décision dans le cadre de ce mécanisme de guichet unique.

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

(129) Afin de veiller à faire appliquer le présent règlement et à contrôler son application de manière cohérente dans l'ensemble de l'Union, les autorités de contrôle devraient avoir, dans chaque État membre, les mêmes missions et les mêmes pouvoirs effectifs, y compris les pouvoirs d'enquête, le pouvoir d'adopter des mesures correctrices et d'infliger des sanctions, ainsi que le pouvoir d'autoriser et d'émettre des avis consultatifs, notamment en cas de réclamation introduite par des personnes physiques, et, sans préjudice des pouvoirs des autorités chargées des poursuites en vertu du droit d'un État membre, le pouvoir de porter les violations du présent règlement à l'attention des autorités judiciaires et d'ester en justice. Ces pouvoirs devraient également inclure celui d'imposer une limitation temporaire ou définitive au traitement, y compris une interdiction. Les États membres peuvent préciser d'autres missions liées à la protection des données à caractère personnel en application du présent règlement. Les pouvoirs des autorités de contrôle devraient être exercés conformément aux garanties procédurales appropriées prévues par le droit de l'Union et le droit des État membres, d'une manière impartiale et équitable et dans un délai raisonnable. Toute mesure devrait notamment être appropriée, nécessaire et proportionnée en vue de garantir le respect du présent règlement, compte tenu des circonstances de l'espèce, respecter le droit de chacun à être entendu avant que soit prise toute mesure individuelle susceptible de lui porter atteinte et éviter les coûts superflus ainsi que les désagréments excessifs pour les personnes concernées. Les pouvoirs d'enquête en ce qui concerne l'accès aux installations devraient être exercés conformément aux exigences spécifiques du droit procédural des États membres, telle que l'obligation d'obtenir une autorisation judiciaire préalable. Toute mesure juridiquement contraignante prise par l'autorité de contrôle devrait être présentée par écrit, être claire et dénuée d'ambiguïté, indiquer quelle autorité de contrôle a pris la mesure et à quelle date, porter la signature du chef ou d'un membre de l'autorité de contrôle qu'il a autorisé, exposer les motifs qui sous-tendent la mesure et mentionner le droit à un recours effectif. Cela ne devrait pas exclure des exigences supplémentaires prévues par le droit procédural des États membres. Si une décision juridiquement contraignante est adoptée, elle peut donner lieu à un contrôle juridictionnel dans l'État membre dont relève l'autorité de contrôle qui l'a adoptée.

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

(131) Lorsqu'une autre autorité de contrôle devrait faire office d'autorité de contrôle chef de file pour les activités de traitement du responsable du traitement ou du sous-traitant mais que l'objet concret d'une réclamation ou la violation éventuelle ne concerne que les activités de traitement du responsable du traitement ou du sous-traitant dans l'État membre dans lequel la réclamation a été introduite ou dans lequel la violation éventuelle a été constatée et que la question n'affecte pas sensiblement ou n'est pas susceptible d'affecter sensiblement des personnes concernées dans d'autres États membres, l'autorité de contrôle qui est saisie d'une réclamation, ou qui constate des situations susceptibles de constituer des violations du présent règlement ou qui est informée d'une autre manière de telles situations devrait rechercher un règlement amiable avec le responsable du traitement et, en cas d'échec, exercer l'ensemble de ses pouvoirs. Ceci devrait comprendre: les traitements spécifiques qui sont effectués sur le territoire de l'État membre dont relève l'autorité de contrôle ou qui portent sur des personnes concernées se trouvant sur le territoire de cet État membre; les traitements effectués dans le cadre d'une offre de biens ou de services visant spécifiquement des personnes concernées se trouvant sur le territoire de l'État membre dont relève l'autorité de contrôle; ou encore les traitements qui doivent être évalués à l'aune des obligations légales pertinentes prévues par le droit d'un État membre.

(132) Les activités de sensibilisation organisées par les autorités de contrôle à l'intention du public devraient comprendre des mesures spécifiques destinées aux responsables du traitement et aux sous-traitants, y compris les micro, petites et moyennes entreprises, ainsi qu'aux personnes physiques, notamment dans le cadre éducatif.

(133) Les autorités de contrôle devraient s'entraider dans l'accomplissement de leurs missions et se prêter mutuellement assistance afin de faire appliquer le présent règlement et de contrôler son application de manière cohérente dans le marché intérieur. Une autorité de contrôle qui fait appel à l'assistance mutuelle peut adopter une mesure provisoire si elle ne reçoit pas de réponse à sa demande d'assistance mutuelle dans un délai d'un mois à compter de la réception de la demande d'assistance mutuelle par l'autre autorité de contrôle.

(134) Chaque autorité de contrôle devrait, s'il y a lieu, participer à des opérations conjointes avec d'autorités de contrôle. L'autorité de contrôle requise devrait être tenue de répondre à la demande dans un délai déterminé.

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

(136) Dans le cadre de l'application du mécanisme de contrôle de la cohérence, le comité devrait émettre un avis, dans un délai déterminé, si une majorité de ses membres le décide ou s'il est saisi d'une demande en ce sens par une autorité de contrôle concernée ou par la Commission. Le comité devrait également être habilité à adopter des décisions juridiquement contraignantes en cas de litiges entre autorités de contrôle. À cet effet, il devrait prendre, en principe à la majorité des deux tiers de ses membres, des décisions juridiquement contraignantes dans des cas clairement définis, en cas de points de vue divergents parmi les autorités de contrôle, notamment dans le cadre du mécanisme de coopération entre l'autorité de contrôle chef de file et les autorités de contrôle concernées, sur le fond de l'affaire et en particulier sur la question de savoir s'il y a ou non violation du présent règlement.

(137) Il peut être nécessaire d'intervenir en urgence pour protéger les droits et libertés des personnes concernées, en particulier lorsque le danger existe que l'exercice du droit d'une personne concernée pourrait être considérablement entravé. En conséquence, une autorité de contrôle devrait pouvoir adopter, sur son territoire, des mesures provisoires dûment justifiées et d'une durée de validité déterminée qui ne devrait pas excéder trois mois.

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

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

(140) Le comité devrait être assisté par un secrétariat assuré par le Contrôleur européen de la protection des données. Pour s'acquitter de ses tâches, le personnel du Contrôleur européen de la protection des données chargé des missions que le présent règlement confie au comité ne devrait recevoir d'instructions que du président du comité et devrait être placé sous l'autorité de celui-ci.

(141) Toute personne concernée devrait avoir le droit d'introduire une réclamation auprès d'une seule autorité de contrôle, en particulier dans l'État membre où elle a sa résidence habituelle, et disposer du droit à un recours

juridictionnel effectif conformément à l'article 47 de la Charte si elle estime que les droits que lui confère le présent règlement sont violés ou si l'autorité de contrôle ne donne pas suite à sa réclamation, la refuse ou la rejette, en tout ou en partie, ou si elle n'agit pas alors qu'une action est nécessaire pour protéger les droits de la personne concernée. L'enquête faisant suite à une réclamation devrait être menée, sous contrôle juridictionnel, dans la mesure appropriée requise par le cas d'espèce. L'autorité de contrôle devrait informer la personne concernée de l'état d'avancement et de l'issue de la réclamation dans un délai raisonnable. Si l'affaire requiert un complément d'enquête ou une coordination avec une autre autorité de contrôle, des informations intermédiaires devraient être fournies à la personne concernée. Afin de faciliter l'introduction des réclamations, chaque autorité de contrôle devrait prendre des mesures telles que la fourniture d'un formulaire de réclamation qui peut être également rempli par voie électronique, sans que d'autres moyens de communication soient exclus.

(142) Lorsqu'une personne concernée estime que les droits que lui confère le présent règlement sont violés, elle devrait avoir le droit de mandater un organisme, une organisation ou une association à but non lucratif, constitué conformément au droit 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 d'une autorité de contrôle, exerce le droit à un recours juridictionnel au nom de personnes concernées ou, si cela est prévu par le droit d'un État membre, exerce le droit d'obtenir réparation au nom de personnes concernées. Un État membre peut prévoir que cet organisme, cette organisation ou cette association a le droit d'introduire une réclamation dans cet État membre, indépendamment de tout mandat confié par une personne concernée, et dispose du droit à un recours juridictionnel effectif s'il a des raisons de considérer que les droits d'une personne concernée ont été violés parce que le traitement des données à caractère personnel a eu lieu en violation du présent règlement. Cet organisme, cette organisation ou cette association ne peut pas être autorisé à réclamer réparation pour le compte d'une personne concernée indépendamment du mandat confié par la personne concernée.

(143) Toute personne physique ou morale a le droit de former un recours en annulation des décisions du comité devant la Cour de justice dans les conditions prévues à l'article 263 du traité sur le fonctionnement de l'Union européenne. Dès lors qu'elles reçoivent de telles décisions, les autorités de contrôle concernées qui souhaitent les contester doivent le faire dans un délai de deux mois à compter de la notification qui leur en a été faite, conformément à l'article 263 du traité sur le fonctionnement de l'Union européenne. Lorsque des décisions du comité concernent directement et individuellement un responsable du traitement, un sous-traitant ou l'auteur de la réclamation, ces derniers peuvent former un recours en annulation de ces décisions dans un délai de deux mois à compter de leur publication sur le site internet du comité, conformément à l'article 263 du traité sur le fonctionnement de l'Union européenne. Sans préjudice de ce droit prévu à l'article 263 du traité sur le fonctionnement de l'Union européenne, toute personne physique ou morale devrait disposer d'un recours juridictionnel effectif, devant la juridiction nationale compétente, contre une décision d'une autorité de contrôle qui produit des effets juridiques à son égard. Une telle décision concerne en particulier l'exercice, par l'autorité de contrôle, de pouvoirs d'enquête, d'adoption de mesures correctrices et d'autorisation ou le refus ou le rejet de réclamations. Toutefois, ce droit à un recours juridictionnel effectif ne couvre pas des mesures prises par les autorités de contrôle qui ne sont pas juridiquement contraignantes, telles que les avis émis ou les conseils fournis par une autorité de contrôle. Les actions contre une autorité de contrôle devraient être portées devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie et être menées conformément au droit procédural de cet État membre. Ces juridictions devraient disposer d'une pleine compétence, et notamment de celle d'examiner toutes les questions de fait et de droit relatives au litige dont elles sont saisies.

Lorsqu'une réclamation a été rejetée ou refusée par une autorité de contrôle, l'auteur de la réclamation peut intenter une action devant les juridictions de ce même État membre. Dans le cadre des recours juridictionnels relatifs à l'application du présent règlement, les juridictions nationales qui estiment qu'une décision sur la question est nécessaire pour leur permettre de rendre leur jugement peuvent ou, dans le cas prévu à l'article 267 du traité sur le fonctionnement de l'Union européenne, doivent demander à la Cour de justice de statuer à titre préjudiciel sur l'interprétation du droit de l'Union, y compris le présent règlement. En outre, lorsqu'une décision d'une autorité de contrôle mettant en œuvre une décision du comité est contestée devant une juridiction nationale et que la validité de la décision du comité est en cause, ladite juridiction nationale n'est pas habilitée à invalider la décision du comité et doit, dans tous les cas où elle considère qu'une décision est invalide, soumettre la question de la validité à la Cour de justice, conformément à l'article 267 du traité sur le fonctionnement de l'Union européenne tel qu'il a été interprété par la Cour de justice. Toutefois, une juridiction nationale peut ne pas soumettre une question relative à la validité d'une décision du comité à la demande d'une personne physique ou morale qui a eu la possibilité de former un recours en annulation de cette décision, en particulier si elle était concernée directement et individuellement par ladite décision, et ne l'a pas fait dans le délai prévu à l'article 263 du traité sur le fonctionnement de l'Union européenne.

(144) Lorsqu'une juridiction saisie d'une action contre une décision prise par une autorité de contrôle a des raisons de croire que des actions concernant le même traitement, portant par exemple sur le même objet, effectué par le même responsable du traitement ou le même sous-traitant, ou encore la même cause, sont introduites devant une juridiction compétente d'un autre État membre, il convient qu'elle contacte cette autre juridiction afin de confirmer l'existence de telles actions connexes. Si des actions connexes sont pendantes devant une juridiction

d'un autre État membre, toute juridiction autre que celle qui a été saisie en premier peut surseoir à statuer ou peut, à la demande de l'une des parties, se dessaisir au profit de la juridiction saisie en premier si celle-ci est compétente pour connaître de l'action concernée et que le droit dont elle relève permet de regrouper de telles actions connexes. Sont réputées connexes, les actions qui sont à ce point étroitement liées qu'il y a intérêt à les instruire et à les juger en même temps afin d'éviter que ne soient rendues des décisions inconciliables, issues de procédures séparées.

(145) En ce qui concerne les actions contre un responsable du traitement ou un sous-traitant, le demandeur devrait pouvoir choisir d'intenter l'action devant les juridictions des États membres dans lesquels le responsable du traitement ou le sous-traitant dispose d'un établissement ou dans l'État membre dans lequel la personne concernée réside, à moins que le responsable du traitement ne soit une autorité publique d'un État membre agissant dans l'exercice de ses prérogatives de puissance publique.

(146) Le responsable du traitement ou le sous-traitant devrait réparer tout dommage qu'une personne peut subir du fait d'un traitement effectué en violation du présent règlement. Le responsable du traitement ou le sous-traitant devrait être exonéré de sa responsabilité s'il prouve que le dommage ne lui est nullement imputable. La notion de dommage devrait être interprétée au sens large, à la lumière de la jurisprudence de la Cour de justice, d'une manière qui tienne pleinement compte des objectifs du présent règlement. Cela est sans préjudice de toute action en dommages-intérêts fondée sur une infraction à d'autres règles du droit de l'Union ou du droit d'un État membre. Un traitement effectué en violation du présent règlement comprend aussi un traitement effectué en violation des actes délégués et d'exécution adoptés conformément au présent règlement et au droit d'un État membre précisant les règles du présent règlement. Les personnes concernées devraient recevoir une réparation complète et effective pour le dommage subi. Lorsque des responsables du traitement ou des sous-traitants participent à un même traitement, chaque responsable du traitement ou chaque sous-traitant devrait être tenu responsable pour la totalité du dommage. Toutefois, lorsque des responsables du traitement et des sous-traitants sont concernés par la même procédure judiciaire, conformément au droit d'un État membre, la réparation peut être répartie en fonction de la part de responsabilité de chaque responsable du traitement ou de chaque sous-traitant dans le dommage causé par le traitement, à condition que le dommage subi par la personne concernée soit entièrement et effectivement réparé. Tout responsable du traitement ou tout sous-traitant qui a réparé totalement le dommage peut par la suite introduire un recours contre d'autres responsables du traitement ou sous-traitants ayant participé au même traitement.

(147) Lorsque le présent règlement prévoit des règles de compétence spécifiques, notamment en ce qui concerne les procédures relatives aux recours juridictionnels, y compris ceux qui visent à obtenir réparation, contre un responsable du traitement ou un sous-traitant, les règles de compétence générales, telles que celles prévues dans le règlement (UE) n° 1215/2012 du Parlement européen et du Conseil ([1]), ne devraient pas porter préjudice à l'application de telles règles juridictionnelles spécifiques.

(148) Afin de renforcer l'application des règles du présent règlement, des sanctions y compris des amendes administratives devraient être infligées pour toute violation du présent règlement, en complément ou à la place des mesures appropriées imposées par l'autorité de contrôle en vertu du présent règlement. En cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende. Il convient toutefois de tenir dûment compte de la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant, de l'application d'un code de conduite, et de toute autre circonstance aggravante ou atténuante. L'application de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la Charte, y compris le droit à une protection juridictionnelle effective et à une procédure régulière.

(149) Les États membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violation du présent règlement, y compris de violation des dispositions nationales adoptées en application et dans les limites du présent règlement. Ces sanctions pénales peuvent aussi permettre la saisie des profits réalisés en violation du présent règlement. Toutefois, l'application de sanctions pénales en cas de violation de ces dispositions nationales et l'application de sanctions administratives ne devrait pas entraîner la violation du principe *ne bis in idem* tel qu'il a été interprété par la Cour de justice.

(150) Afin de renforcer et d'harmoniser les sanctions administratives applicables en cas de violation du présent règlement, chaque autorité de contrôle devrait avoir le pouvoir d'imposer des amendes administratives. Le présent

([1]) Règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (JO L 351 du 20.12.2012, p. 1).

règlement devrait définir les violations, le montant maximal et les critères de fixation des amendes administratives dont elles sont passibles, qui devraient être fixés par l'autorité de contrôle compétente dans chaque cas d'espèce, en prenant en considération toutes les caractéristiques propres à chaque cas et compte dûment tenu, notamment, 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 règlement et pour prévenir ou atténuer les conséquences de la violation. Lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Lorsque des amendes administratives sont imposées à des personnes qui ne sont pas une entreprise, l'autorité de contrôle devrait tenir compte, lorsqu'elle examine quel serait le montant approprié de l'amende, du niveau général des revenus dans l'État membre ainsi que de la situation économique de la personne en cause. Il peut en outre être recouru au mécanisme de contrôle de la cohérence pour favoriser une application cohérente des amendes administratives. Il devrait appartenir aux États membres de déterminer si et dans quelle mesure les autorités publiques devraient faire l'objet d'amendes administratives. L'application d'une amende administrative ou le fait de donner un avertissement ne portent pas atteinte à l'exercice d'autres pouvoirs des autorités de contrôle ou à l'application d'autres sanctions en vertu du présent règlement.

(151) Les systèmes juridiques du Danemark et de l'Estonie ne permettent pas d'imposer des amendes administratives comme le prévoit le présent règlement. Les règles relatives aux amendes administratives peuvent être appliquées de telle sorte que, au Danemark, l'amende est imposée par les juridictions nationales compétentes sous la forme d'une sanction pénale et en Estonie, l'amende est imposée par l'autorité de contrôle dans le cadre d'une procédure de délit, à condition qu'une telle application des règles dans ces États membres ait un effet équivalent aux amendes administratives imposées par les autorités de contrôle. C'est pourquoi les juridictions nationales compétentes devraient tenir compte de la recommandation formulée par l'autorité de contrôle qui est à l'origine de l'amende. En tout état de cause, les amendes imposées devraient être effectives, proportionnées et dissuasives.

(152) Lorsque le présent règlement n'harmonise pas les sanctions administratives ou, si nécessaire dans d'autres circonstances, par exemple en cas de violation grave du présent règlement, les États membres devraient mettre en œuvre un système qui prévoit des sanctions effectives, proportionnées et dissuasives. La nature de ces sanctions, pénales ou administratives, devrait être déterminée par le droit des États membres.

(153) Le droit des États membres devrait concilier les règles régissant la liberté d'expression et d'information, y compris l'expression journalistique, universitaire, artistique ou littéraire, et le droit à la protection des données à caractère personnel en vertu du présent règlement. Dans le cadre du traitement de données à caractère personnel uniquement à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, il y a lieu de prévoir des dérogations ou des exemptions à certaines dispositions du présent règlement si cela est nécessaire pour concilier le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, consacré par l'article 11 de la Charte. Tel devrait notamment être le cas des traitements de données à caractère personnel dans le domaine de l'audiovisuel et dans les documents d'archives d'actualités et bibliothèques de la presse. En conséquence, les États membres devraient adopter des dispositions législatives qui fixent les exemptions et dérogations nécessaires aux fins d'assurer un équilibre entre ces droits fondamentaux. Les États membres devraient adopter de telles exemptions et dérogations en ce qui concerne les principes généraux, les droits de la personne concernée, le responsable du traitement et le sous-traitant, le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, les autorités de contrôle indépendantes, la coopération et la cohérence, ainsi que les situations particulières de traitement des données. Lorsque ces exemptions ou dérogations diffèrent d'un État membre à l'autre, le droit de l'État membre dont relève le responsable du traitement devrait s'appliquer. Pour tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique, il y a lieu de retenir une interprétation large des notions liées à cette liberté, telles que le journalisme.

(154) Le présent règlement permet de prendre en compte, dans son application, le principe de l'accès du public aux documents officiels. L'accès du public aux documents officiels peut être considéré comme étant dans l'intérêt public. Les données à caractère personnel figurant dans des documents détenus par une autorité publique ou un organisme public devraient pouvoir être rendues publiques par ladite autorité ou ledit organisme si cette communication est prévue par le droit de l'Union ou le droit de l'État membre dont relève l'autorité publique ou l'organisme public. Ces dispositions légales devraient concilier l'accès du public aux documents officiels et la réutilisation des informations du secteur public, d'une part, et le droit à la protection des données à caractère personnel, d'autre part, et peuvent dès lors prévoir la conciliation nécessaire avec le droit à la protection des données à caractère personnel en vertu du présent règlement. Dans ce contexte, il convient d'entendre par «autorités publiques et organismes publics», toutes les autorités ou autres organismes relevant du droit d'un État membre en matière d'accès du public aux documents. La directive 2003/98/CE du Parlement européen et du Conseil ([1]) laisse intact et n'affecte en rien le niveau de protection des personnes physiques à l'égard du traitement

([1]) Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public (JO L 345 du 31.12.2003, p. 90).

des données à caractère personnel garanti par les dispositions du droit de l'Union et du droit des États membres et, en particulier, ne modifie en rien les droits et obligations prévus dans le présent règlement. En particulier, ladite directive ne devrait pas s'appliquer aux documents dont l'accès est exclu ou limité en application de règles d'accès pour des motifs de protection des données à caractère personnel, et aux parties de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été prévue par la loi comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

(155) Le droit des États membres ou des conventions collectives, y compris des «accords d'entreprise» peuvent prévoir des règles spécifiques relatives au traitement des données à caractère personnel des employés dans le cadre des relations de travail, notamment les conditions dans lesquelles les données à caractère personnel dans le cadre des relations de travail peuvent être traitées sur la base du consentement de l'employé, aux fins du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, et aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.

(156) Le traitement des données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques devrait être soumis à des garanties appropriées pour les droits et libertés de la personne concernée, en vertu du présent règlement. Ces garanties devraient permettre la mise en place de mesures techniques et organisationnelles pour assurer, en particulier, le respect du principe de minimisation des données. Le traitement ultérieur de données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques doit être effectué lorsque que le responsable du traitement a évalué s'il est possible d'atteindre ces finalités grâce à un traitement de données qui ne permettent pas ou plus d'identifier les personnes concernées, pour autant que des garanties appropriées existent (comme par exemple la pseudonymisation des données). Les États membres devraient prévoir 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. Les États membres devraient être autorisés à prévoir, dans des conditions spécifiques et moyennant des garanties appropriées pour les personnes concernées, des dispositions particulières et des dérogations concernant les exigences en matière d'information et les droits à la rectification, à l'effacement, à l'oubli, à la limitation du traitement, à la portabilité des données et le droit d'opposition lorsque les données à caractère personnel sont traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Les conditions et garanties en question peuvent comporter des procédures spécifiques permettant aux personnes concernées d'exercer ces droits si cela est approprié eu égard aux finalités du traitement spécifique concerné, ainsi que des mesures techniques et organisationnelles visant à réduire à un minimum le traitement des données à caractère personnel conformément aux principes de proportionnalité et de nécessité. Le traitement de données à caractère personnel à des fins scientifiques devrait également respecter d'autres dispositions législatives pertinentes, telles que celles relatives aux essais cliniques.

(157) En combinant les informations issues des registres, les chercheurs peuvent acquérir de nouvelles connaissances d'un grand intérêt en ce qui concerne des problèmes médicaux très répandus tels que les maladies cardiovasculaires, le cancer et la dépression. Sur la base des registres, les résultats de la recherche peuvent être améliorés car ils s'appuient sur un échantillon plus large de population. Dans le cadre des sciences sociales, la recherche sur la base des registres permet aux chercheurs d'acquérir des connaissances essentielles sur les corrélations à long terme existant entre un certain nombre de conditions sociales telles que le chômage et l'éducation et d'autres conditions de vie. Les résultats de la recherche obtenus à l'aide des registres fournissent des connaissances fiables et de grande qualité qui peuvent servir de base à l'élaboration et à la mise en œuvre d'une politique fondée sur la connaissance, améliorer la qualité de vie d'un certain nombre de personnes et renforcer l'efficacité des services sociaux. Pour faciliter la recherche scientifique, les données à caractère personnel peuvent être traitées à des fins de recherche scientifique sous réserve de conditions et de garanties appropriées prévues dans le droit de l'Union ou le droit des États membres.

(158) Lorsque les données à caractère personnel sont traitées à des fins archivistiques, le présent règlement devrait également s'appliquer à ce traitement, étant entendu qu'il ne devrait pas s'appliquer aux des personnes décédées. Les autorités publiques ou les organismes publics ou privés qui conservent des archives dans l'intérêt public devraient être des services qui, en vertu du droit de l'Union ou du droit d'un État membre, ont l'obligation légale de collecter, de conserver, d'évaluer, d'organiser, de décrire, de communiquer, de mettre en valeur, de diffuser des archives qui sont à conserver à titre définitif dans l'intérêt public général et d'y donner accès. Les États membres devraient également être autorisés à prévoir un traitement ultérieur des données à caractère personnel à des fins archivistiques, par exemple en vue de fournir des informations précises relatives au comportement politique sous les régimes des anciens États totalitaires, aux génocides, aux crimes contre l'humanité, notamment l'Holocauste, ou aux crimes de guerre.

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

(160) Lorsque des données à caractère personnel sont traitées à des fins de recherche historique, le présent règlement devrait également s'appliquer à ce traitement. Cela devrait aussi comprendre les recherches historiques et les recherches à des fins généalogiques, étant entendu que le présent règlement ne devrait pas s'appliquer aux personnes décédées.

(161) Aux fins du consentement à la participation à des activités de recherche scientifique dans le cadre d'essais cliniques, les dispositions pertinentes du règlement (UE) nº 536/2014 du Parlement européen et du Conseil ([1]) devraient s'appliquer.

(162) Lorsque des données à caractère personnel sont traitées à des fins statistiques, le présent règlement devrait s'appliquer à ce traitement. Le droit de l'Union ou le droit des États membres devrait, dans les limites du présent règlement, déterminer le contenu statistique, définir le contrôle de l'accès aux données et arrêter des dispositions particulières pour le traitement de données à caractère personnel à des fins statistiques ainsi que des mesures appropriées pour la sauvegarde des droits et libertés de la personne concernée et pour préserver le secret statistique. Par «fins statistiques», on entend toute opération de collecte et de traitement de données à caractère personnel nécessaires pour des enquêtes statistiques ou la production de résultats statistiques. Ces résultats statistiques peuvent en outre être utilisés à différentes fins, notamment des fins de recherche scientifique. Les fins statistiques impliquent que le résultat du traitement à des fins statistiques ne constitue pas des données à caractère personnel mais des données agrégées, et que ce résultat ou ces données à caractère personnel ne sont pas utilisés à l'appui de mesures ou de décisions concernant une personne physique en particulier.

(163) Les informations confidentielles que les autorités statistiques de l'Union et des États membres recueillent pour élaborer des statistiques officielles européennes et nationales devraient être protégées. Les statistiques européennes devraient être mises au point, élaborées et diffusées conformément aux principes statistiques énoncés à l'article 338, paragraphe 2, du traité sur le fonctionnement de l'Union européenne, et les statistiques nationales devraient également respecter le droit des États membres. Le règlement (CE) nº 223/2009 du Parlement européen et du Conseil ([2]) contient d'autres dispositions particulières relatives aux statistiques européennes couvertes par le secret.

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

(165) Le présent règlement respecte et ne porte pas préjudice au statut dont bénéficient, en vertu du droit constitutionnel en vigueur, les églises et les associations ou communautés religieuses dans les États membres, tel qu'il est reconnu par l'article 17 du traité sur le fonctionnement de l'Union européenne.

(166) Afin de remplir les objectifs du présent règlement, à savoir protéger les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel, et garantir la

([1]) Règlement (UE) nº 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE (JO L 158 du 27.5.2014, p. 1).

([2]) Règlement (CE) nº 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) nº 1101/2008 du Parlement européen et du Conseil relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) nº 322/97 du Conseil relatif à la statistique communautaire et la décision 89/382/CEE, Euratom du Conseil instituant un comité du programme statistique des Communautés européennes (JO L 87 du 31.3.2009, p. 164).

libre circulation de ces données au sein de l'Union, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne. En particulier, des actes délégués devraient être adoptés en ce qui concerne les critères et exigences applicables aux mécanismes de certification, les informations à présenter sous la forme d'icônes normalisées ainsi que les procédures régissant la fourniture de ces icônes. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts. Il convient que, lorsqu'elle prépare et élabore des actes délégués, la Commission veille à ce que tous les documents pertinents soient transmis simultanément en temps utile et de façon appropriée au Parlement européen et au Conseil.

(167) 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. Dans ce cadre, la Commission devrait envisager des mesures spécifiques pour les micro, petites et moyennes entreprises.

(168) Compte tenu de la portée générale des actes concernés, il convient d'avoir recours à la procédure d'examen pour l'adoption d'actes d'exécution en ce qui concerne les clauses contractuelles types entre les responsables du traitement et les sous-traitants ainsi qu'entre les sous-traitants; des codes de conduite; des normes techniques et des mécanismes de certification; le niveau adéquat de protection offert par un pays tiers, un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale; les clauses types de protection; les formats et les procédures pour l'échange d'informations par voie électronique entre responsables du traitement, sous-traitants et autorités de contrôle en ce qui concerne les règles d'entreprise contraignantes; l'assistance mutuelle; et les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle ainsi qu'entre les autorités de contrôle et le comité.

(169) La Commission devrait adopter des actes d'exécution immédiatement applicables lorsque les éléments de preuve disponibles montrent qu'un pays tiers, un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale n'offre pas un niveau de protection adéquat et que des raisons d'urgence impérieuses l'imposent.

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

(171) La directive 95/46/CE devrait être abrogée par le présent règlement. Les traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur. Lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable du traitement puisse poursuivre le traitement après la date d'application du présent règlement. Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées.

(172) 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 un avis le 7 mars 2012 ([1]).

(173) Le présent règlement devrait s'appliquer à tous les aspects de la protection des libertés et droits fondamentaux à l'égard du traitement des données à caractère personnel qui ne sont pas soumis à des obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE du Parlement européen et du Conseil ([2]), y compris les obligations incombant au responsable du traitement et les droits des personnes physiques. Afin de clarifier la relation entre le présent règlement et la directive 2002/58/CE, cette directive devrait être modifiée en conséquence. Après l'adoption du présent règlement, il convient de réexaminer la directive 2002/58/CE, notamment afin d'assurer la cohérence avec le présent règlement,

([1]) JO C 192 du 30.6.2012, p. 7.
([2]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

Dispositions générales

Article premier

Objet et objectifs

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

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

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

Article 2

Champ d'application matériel

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

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

a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union;

b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne;

c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique;

d) 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 des menaces pour la sécurité publique et la prévention de telles menaces.

3. Le règlement (CE) nº 45/2001 s'applique au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union. Le règlement (CE) nº 45/2001 et les autres actes juridiques de l'Union applicables audit traitement des données à caractère personnel sont adaptés aux principes et aux règles du présent règlement conformément à l'article 98.

4. Le présent règlement s'applique sans préjudice de la directive 2000/31/CE, et notamment de ses articles 12 à 15 relatifs à la responsabilité des prestataires de services intermédiaires.

Article 3

Champ d'application territorial

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

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

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou

b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

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

Article 4

Définitions

Aux fins du présent règlement, on entend par:

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

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

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

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

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

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

7) «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

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

9) «destinataire», la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques

qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement;

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

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

12) «violation de données à caractère personnel», une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

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

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

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

16) «établissement principal»,

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

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

17) «représentant», une personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du présent règlement;

18) «entreprise», une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique;

19) «groupe d'entreprises», une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle;

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

21) «autorité de contrôle», une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51;

22) «autorité de contrôle concernée», une autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que:

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

b) des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être; ou

c) une réclamation a été introduite auprès de cette autorité de contrôle;

23) «traitement transfrontalier»,

a) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres; ou

b) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres;

24) «objection pertinente et motivée», une objection à un projet de décision quant à savoir s'il y a ou non violation du présent règlement ou si l'action envisagée en ce qui concerne le responsable du traitement ou le sous-traitant respecte le présent règlement, qui démontre clairement l'importance des risques que présente le projet de décision pour les libertés et droits fondamentaux des personnes concernées et, le cas échéant, le libre flux des données à caractère personnel au sein de l'Union;

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

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

CHAPITRE II

Principes

Article 5

Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être:

a) traitées de manière licite, 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 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

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

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

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

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 89, paragraphe 1, 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 6

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

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

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

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

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

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

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

2. Les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX.

3. Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par:

a) le droit de l'Union; ou

b) le droit de l'État membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires 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. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de

traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi.

4. Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, 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 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10;

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 6, paragraphe 1, point a), 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 16 ans. Lorsque l'enfant est âgé de moins de 16 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.

Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.

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

Traitement portant sur des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

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

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre 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 physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;

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

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

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

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un 'État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée;

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit 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, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

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

4. Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé.

Article 10

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

Le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un 'État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

Article 11

Traitement ne nécessitant pas l'identification

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

2. Lorsque, dans les cas visés au paragraphe 1 du présent article, le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il en informe la personne concernée, si possible. En pareils cas, les articles 15 à 20 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.

CHAPITRE III

Droits de la personne concernée

Section 1

Transparence et modalités

Article 12

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

1. Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

2. Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22. Dans les cas visés à l'article 11, paragraphe 2, le responsable du traitement ne refuse pas de donner suite à la demande de la personne concernée d'exercer les droits que lui confèrent les articles 15 à 22, à moins que le responsable du traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée.

3. Le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22, 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 d'une autorité de contrôle et de former un recours juridictionnel.

5. Aucun paiement n'est exigé pour fournir les informations au titre des articles 13 et 14 et pour procéder à toute communication et prendre toute mesure au titre des articles 15 à 22 et de l'article 34. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut:

a) exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées; ou

b) refuser de donner suite à ces demandes.

Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

6. Sans préjudice de l'article 11, lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée aux articles 15 à 21, 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 13 et 14 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. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 92, aux fins de déterminer les informations à présenter sous la forme d'icônes ainsi que les procédures régissant la fourniture d'icônes normalisées.

Section 2

Information et accès aux données à caractère personnel

Article 13

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 et, le cas échéant, du représentant du responsable du traitement

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

e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent; et

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition;

2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent:

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

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

c) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer 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 d'une autorité de contrôle;

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 éventuelles de la non-fourniture de ces données;

f) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, 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 les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

4. Les paragraphes 1, 2 et 3 ne s'appliquent pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations.

Article 14

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 et, le cas échéant, du représentant du responsable du traitement;

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

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

d) les catégories de données à caractère personnel concernées;

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

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition;

2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée les informations 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) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;

c) 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, ainsi que du droit de s'opposer au traitement et du droit à la portabilité des données;

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

e) le droit d'introduire une réclamation auprès d'une autorité de contrôle;

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

g) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

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

a) dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées;

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

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

4. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

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

a) la personne concernée dispose déjà de ces informations;

b) la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve des conditions et garanties visées à l'article 89, paragraphe 1, ou dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles;

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

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

Article 15

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 d'une autorité de contrôle;

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

h) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, 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, en vertu de l'article 46, 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. Le responsable du traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement.

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

Section 3

Rectification et effacement

Article 16

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 17

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 6, paragraphe 1, point a), ou à l'article 9, 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 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2;

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 qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis;

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

2. Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement 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 qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3;

d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou

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

Article 18

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 des données à caractère personnel;

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

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

d) la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

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

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

Article 19

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 effectué conformément à l'article 16, à l'article 17, paragraphe 1, et à l'article 18, 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 20

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

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

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

3. L'exercice du droit, visé au paragraphe 1 du présent article s'entend sans préjudice de l'article 17. Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

4. Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés de tiers.

Section 4

Droit d'opposition et prise de décision individuelle automatisée

Article 21

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 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. 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. Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection.

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

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

5. Dans le cadre de l'utilisation de services de la société de l'information, et nonobstant la directive 2002/58/CE, la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.

6. Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques en application de l'article 89, paragraphe 1, 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 22

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 un responsable du traitement;

b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée; ou

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

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

4. Les décisions visées au paragraphe 2 ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, à moins que l'article 9, 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 23

Limitations

1. Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 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;

b) la défense nationale;

c) la sécurité publique;

d) 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;

e) 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;

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

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

h) une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g);

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

j) l'exécution des demandes de droit civil.

2. En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant:

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

b) aux catégories de données à caractère personnel;

c) à l'étendue des limitations introduites;

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

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

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

g) aux risques pour les droits et libertés des personnes concernées; et

h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation.

CHAPITRE IV

Responsable du traitement et sous-traitant

Section 1

Obligations générales

Article 24

Responsabilité du responsable du traitement

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

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

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

Article 25

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

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

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

3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

Article 26

Responsables conjoints du traitement

1. Lorsque deux responsables du traitement ou plus 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 obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations 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 visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

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

Article 27

Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union

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

2. L'obligation prévue au paragraphe 1 du présent article ne s'applique pas:

a) à un traitement qui est occasionnel, qui n'implique pas un traitement à grande échelle des catégories particulières de données visées à l'article 9, paragraphe 1, ou un traitement de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10, et qui n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement; ou

b) à une autorité publique ou à un organisme public;

3. Le représentant est établi dans un des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement lié à l'offre de biens ou de services, ou dont le comportement fait l'objet d'un suivi.

4. Le représentant est mandaté par le responsable du traitement ou le sous-traitant pour être la personne à qui, notamment, les autorités de contrôle et les personnes concernées doivent s'adresser, en plus ou à la place du responsable du traitement ou du sous-traitant, pour toutes les questions relatives au traitement, aux fins d'assurer le respect du présent règlement.

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

Article 28

Sous-traitant

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

2. Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

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

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant 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 32;

d) respecte les conditions visées 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 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant;

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

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

En ce qui concerne le 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 au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière 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. L'application, par un sous-traitant, d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer l'existence des garanties suffisantes conformément aux paragraphes 1 et 4 du présent article.

6. Sans préjudice d'un contrat particulier entre le responsable du traitement et le sous-traitant, le contrat ou l'autre acte juridique visé aux paragraphes 3 et 4 du présent article peut être fondé, en tout ou en partie, sur les clauses contractuelles types visées aux paragraphes 7 et 8 du présent article, y compris lorsqu'elles font partie d'une certification délivrée au responsable du traitement ou au sous-traitant en vertu des articles 42 et 43.

7. La Commission peut établir des clauses contractuelles types pour les questions visées aux paragraphes 3 et 4 du présent article et conformément à la procédure d'examen visée à l'article 93, paragraphe 2.

8. Une autorité de contrôle peut adopter des clauses contractuelles types pour les questions visées aux paragraphes 3 et 4 du présent article et conformément au mécanisme de contrôle de la cohérence visé à l'article 63.

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

10. Sans préjudice des articles 82, 83 et 84, 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 29

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

Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre.

Article 30

Registre des activités de traitement

1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:

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

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 des pays tiers ou des organisations internationales;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

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

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent 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 et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données;

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

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

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

4. Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande.

5. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Article 31

Coopération avec l'autorité de contrôle

Le responsable du traitement et le sous-traitant ainsi que, le cas échéant, leurs représentants coopèrent avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions.

Section 2

Sécurité des données à.caractère personnel

Article 32

Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

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

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

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

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

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

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

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

Article 33

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

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, 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 à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

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

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

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

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

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

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

5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

Article 34

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

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

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

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

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

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

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

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

Section 3

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

Article 35

Analyse d'impact relative à la protection des données

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

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

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

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

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou

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

4. L'autorité de contrôle 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 conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68.

5. L'autorité de contrôle 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. L'autorité de contrôle communique cette liste au comité.

6. Avant d'adopter les listes visées aux paragraphes 4 et 5, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.

7. L'analyse contient au moins:

a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable 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 conformément au paragraphe 1; et

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

8. Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

9. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

10. Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente 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 dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

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

Article 36

Consultation préalable

1. Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

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

3. Lorsque le responsable du traitement consulte l'autorité de contrôle en application du paragraphe 1, il lui communique:

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

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 en vertu du présent règlement;

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

e) l'analyse d'impact relative à la protection des données prévue à l'article 35; et

f) toute autre information que l'autorité de contrôle demande.

4. Les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement.

5. Nonobstant le paragraphe 1, le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique.

Section 4

Délégué à la protection des données

Article 37

Désignation du délégué à la protection des données

1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

2. Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

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

4. Dans les cas autres que ceux visés au paragraphe 1, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

5. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.

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

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

Article 38

Fonction du délégué à la protection des données

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

2. Le responsable du traitement et le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 39 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées.

3. Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des 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 est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres.

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

Article 39

Missions du délégué à la protection des données

1. Les missions du délégué à la protection des données sont au moins 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 ou du droit des États membres en matière de protection des données;

b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres 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) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35;

d) coopérer avec l'autorité de contrôle;

e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.

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

Section 5

Codes de conduite et certification

Article 40

Codes de conduite

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

2. Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou les proroger, aux fins de préciser les modalités d'application du présent règlement, telles que:

a) le traitement loyal et transparent;

b) les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques;

c) la collecte des données à caractère personnel;

d) la pseudonymisation des données à caractère personnel;

e) les informations communiquées au public et aux personnes concernées;

f) l'exercice des droits des personnes concernées;

g) les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant;

h) les mesures et les procédures visées aux articles 24 et 25 et les mesures visant à assurer la sécurité du traitement visées à l'article 32;

i) la notification aux autorités de contrôle des violations de données à caractère personnel et la communication de ces violations aux personnes concernées;

j) le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales; ou

k) les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement, sans préjudice des droits des personnes concernées au titre des articles 77 et 79.

3. Outre leur application par les responsables du traitement ou les sous-traitants soumis au présent règlement, les codes de conduite qui sont approuvés en vertu du paragraphe 5 du présent article et qui sont d'application générale en vertu du paragraphe 9 du présent article peuvent aussi être appliqués par des responsables du traitement ou des sous-traitants qui ne sont pas soumis au présent règlement en vertu de l'article 3, afin de fournir des garanties appropriées dans le cadre des transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale dans les conditions visées à l'article 46, paragraphe 2, point e). Ces responsables du traitement ou sous-traitants prennent l'engagement contraignant et doté de force obligatoire au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

4. Le code de conduite visé au paragraphe 2 du présent article comprend les mécanismes permettant à l'organisme visé à l'article 41, paragraphe 1, de procéder au contrôle obligatoire du respect de ses dispositions par les responsables du traitement ou les sous-traitants qui s'engagent à l'appliquer, sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56.

5. Les associations et autres organismes visés au paragraphe 2 du présent article qui ont l'intention d'élaborer un code de conduite ou de modifier ou proroger un code de conduite existant soumettent le projet de code, la modifications ou la prorogation à l'autorité de contrôle qui est compétente en vertu de l'article 55. L'autorité de contrôle rend un avis sur la question de savoir si le projet de code, la modification ou la prorogation respecte le présent règlement et approuve ce projet de code, cette modification ou cette prorogation si elle estime qu'il offre des garanties appropriées suffisantes.

6. Lorsque le projet de code, la modification ou la prorogation est approuvé conformément au paragraphe 5, et lorsque le code de conduite concerné ne porte pas sur des activités de traitement menées dans plusieurs États membres, l'autorité de contrôle enregistre et publie le code de conduite.

7. Lorsque le projet de code de conduite concerne des activités de traitement menées dans plusieurs États membres, l'autorité de contrôle qui est compétente en vertu de l'article 55 soumet le projet de code, la modification ou la prorogation, avant approbation, selon la procédure visée à l'article 63, au comité, qui rend un avis sur la question de savoir si le projet de code, la modification ou la prorogation respecte le présent règlement ou, dans la situation visée au paragraphe 3 du présent article, s'il offre des garanties appropriées.

8. Lorsque l'avis visé au paragraphe 7 confirme que le projet de code, la modification ou la prorogation respecte le présent règlement ou, dans la situation visée au paragraphe 3, offre des garanties appropriées, le comité soumet son avis à la Commission.

9. La Commission peut décider, par voie d'actes d'exécution, que le code de conduite, la modification ou la prorogation approuvés qui lui ont été soumis en vertu du paragraphe 8 du présent article sont d'application générale au sein de l'Union. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

10. La Commission veille à garantir une publicité appropriée aux codes approuvés dont elle a décidé qu'ils sont d'application générale conformément au paragraphe 9.

11. Le comité consigne dans un registre tous les codes de conduite, les modifications et les prorogations approuvés et les met à la disposition du public par tout moyen approprié.

Article 41

Suivi des codes de conduite approuvés

1. Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente au titre des articles 57 et 58, le contrôle du respect du code de conduite en vertu de l'article 40 peut être effectué par un organisme qui dispose d'un niveau d'expertise approprié au regard de l'objet du code et qui est agréé à cette fin par l'autorité de contrôle compétente.

2. Un organisme visé au paragraphe 1 peut être agréé pour contrôler le respect d'un code de conduite lorsque cet organisme a:

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

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

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

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

3. L'autorité de contrôle compétente soumet le projet de critères d'agrément d'un organisme visé au paragraphe 1 du présent article au comité en application du mécanisme de contrôle de la cohérence visé à l'article 63.

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

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

6. Le présent article ne s'applique pas au traitement effectué par les autorités publiques et les organismes publics.

Article 42

Certification

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

2. Outre l'application par les responsables du traitement ou les sous-traitants soumis au présent règlement, les mécanismes de certification, les labels ou les marques en matière de protection des données approuvés en vertu du paragraphe 5 du présent article peuvent être établis aux fins de démontrer que des responsables du traitement ou des sous-traitants qui ne sont pas soumis au présent règlement en vertu du l'article 3 fournissent des garanties appropriées dans le cadre des transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale dans les conditions visées à l'article 46, paragraphe 2, point f). Ces responsables du traitement ou sous-traitants prennent l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

3. La certification est volontaire et accessible via un processus transparent.

4. Une certification en vertu du présent article ne diminue par la responsabilité du responsable du traitement ou du sous-traitant quant au respect du présent règlement et est sans préjudice des missions et des pouvoirs des autorités de contrôle qui sont compétentes en vertu de l'article 55 ou 56.

5. Une certification en vertu du présent article est délivrée par les organismes de certification visés à l'article 43 ou par l'autorité de contrôle compétente sur la base des critères approuvés par cette autorité de contrôle compétente en application de l'article 58, paragraphe 3, ou par le comité en application de l'article 63. Lorsque les critères sont approuvés par le comité, cela peut donner lieu à une certification commune, le label européen de protection des données.

6. Le responsable du traitement ou le sous-traitant qui soumet son traitement au mécanisme de certification fournit à l'organisme de certification visé à l'article 43 ou, le cas échéant, à l'autorité de contrôle compétente toutes les informations ainsi que l'accès à ses activités de traitement, qui sont nécessaires pour mener la procédure de certification.

7. La certification est délivrée à un responsable du traitement ou à un sous-traitant pour une durée maximale de trois ans et peut être renouvelée dans les mêmes conditions tant que les exigences applicables continuent d'être satisfaites. La certification est retirée, s'il y a lieu, par les organismes de certification visés à l'article 43 ou par l'autorité de contrôle compétente lorsque les exigences applicables à la certification ne sont pas ou plus satisfaites.

8. Le comité consigne dans un registre tous les mécanismes de certification et les labels ou les marques en matière de protection des données et les met à la disposition du public par tout moyen approprié.

Article 43

Organismes de certification

1. Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente au titre des articles 57 et 58, les organismes de certification disposant d'un niveau d'expertise approprié en matière de protection des données délivrent et renouvellent les certifications, après en avoir informé l'autorité de contrôle pour qu'elle puisse exercer au besoin les pouvoirs qui lui sont dévolus en vertu de l'article 58, paragraphe 2, point h). Les États membres veillent à ce que ces organismes de certification soient agréés par une des entités suivantes ou les deux:

a) l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56;

b) l'organisme national d'accréditation désigné conformément au règlement (CE) nº 765/2008 du Parlement européen et du Conseil ([1]), conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56.

2. Les organismes de certification visés au paragraphe 1 ne sont agréés conformément audit paragraphe que lorsqu'ils ont:

a) démontré, à la satisfaction de l'autorité de contrôle compétente, leur indépendance et leur expertise au regard de l'objet de la certification;

([1]) Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

b) pris l'engagement de respecter les critères visés à l'article 42, paragraphe 5, et approuvés par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56 ou par le comité, en vertu de l'article 63;

c) mis en place des procédures en vue de la délivrance, de l'examen périodique et du retrait d'une certification, de labels et de marques en matière de protection des données;

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

e) démontré, à la satisfaction de l'autorité de contrôle compétente, que leurs tâches et leurs missions n'entraînent pas de conflit d'intérêts.

3. L'agrément des organismes de certification visés aux paragraphes 1 et 2 du présent article se fait sur la base de critères approuvés par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56 ou, par le comité en vertu de l'article 63. En cas d'agrément en application du paragraphe 1, point b), du présent article, ces exigences complètent celles prévues dans le règlement (CE) nº 765/2008 et les règles techniques qui décrivent les méthodes et procédures des organismes de certification.

4. Les organismes de certification visés au paragraphe 1 sont chargés de procéder à l'évaluation appropriée conduisant à la délivrance de la certification ou au retrait de cette certification, sans préjudice de la responsabilité du responsable du traitement ou du sous-traitant en ce qui concerne le respect du présent règlement. L'agrément est délivré pour une durée maximale de cinq ans et peut être renouvelé dans les mêmes conditions tant que l'organisme de certification satisfait aux exigences énoncées au présent article.

5. Les organismes de certification visés au paragraphe 1 communiquent aux autorités de contrôle compétentes les raisons de la délivrance ou du retrait de la certification demandée.

6. Les exigences visées au paragraphe 3 du présent article et les critères visés à l'article 42, paragraphe 5, sont publiés par les autorités de contrôle sous une forme aisément accessible. Les autorités de contrôle transmettent aussi ces exigences et ces critères au comité. Le comité consigne dans un registre tous les mécanismes de certification et les labels en matière de protection des données et les met à la disposition du public par tout moyen approprié.

7. Sans préjudice du chapitre VIII, l'autorité de contrôle compétente ou l'organisme national d'accréditation révoque l'agrément d'un organisme de certification en application du paragraphe 1 du présent article si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organisme de certification constituent une violation du présent règlement.

8. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 92, aux fins de préciser les exigences à prendre en considération en ce qui concerne les mécanismes de certification en matière de protection des données visés à l'article 42, paragraphe 1.

9. La Commission peut adopter des actes d'exécution visant à fixer des normes techniques pour les mécanismes de certification, les labels et les marques en matière de protection des données, ainsi que les mécanismes aux fins de la promotion et de la reconnaissance de ces mécanismes de certification, labels et marques. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

CHAPITRE V

Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales

Article 44

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 45

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 constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

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

a) l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées;

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

c) les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

3. La Commission, après avoir évalué le caractère adéquat du niveau de protection, peut décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, assure un niveau de protection adéquat au sens du paragraphe 2 du présent article. L'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale. L'acte d'exécution précise son champ d'application territorial et sectoriel et, le cas échéant, nomme la ou des autorités de contrôle visées au paragraphe 2, point b), du présent article. L'acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

4. La Commission suit, de manière permanente, les évolutions dans les pays tiers et au sein des organisations internationales qui pourraient porter atteinte au fonctionnement des décisions adoptées en vertu du paragraphe 3 du présent article et des décisions adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE.

5. Lorsque les informations disponibles révèlent, en particulier à l'issue de l'examen visé au paragraphe 3 du présent article, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat au sens du paragraphe 2 du présent article, la Commission si nécessaire, abroge, modifie ou suspend la décision visée au paragraphe 3 du présent article par voie d'actes d'exécution sans effet rétroactif. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

Pour des raisons d'urgence impérieuses dûment justifiées, la Commission adopte des actes d'exécution immédiatement applicables en conformité avec la procédure visée à l'article 93, paragraphe 3.

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

7. Une décision adoptée en vertu du paragraphe 5 du présent article est sans préjudice des transferts de données à caractère personnel vers le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou à l'organisation internationale en question, effectués en application des articles 46 à 49.

8. La Commission publie au *Journal officiel de l'Union européenne* et sur son site internet une liste des pays tiers, des territoires et des secteurs déterminés dans un pays tiers et des organisations internationales pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat est ou n'est plus assuré.

9. Les décisions adoptées par la Commission sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation par une décision de la Commission adoptée conformément au paragraphe 3 ou 5 du présent article.

Article 46

Transferts moyennant des garanties appropriées

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

2. Les garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par:

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

b) des règles d'entreprise contraignantes conformément à l'article 47;

c) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2;

d) des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2;

e) un code de conduite approuvé conformément à l'article 40, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées; ou

f) un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

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

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

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

4. L'autorité de contrôle applique le mécanisme de contrôle de la cohérence visé à l'article 63 dans les cas visés au paragraphe 3 du présent article.

5. Les autorisations accordées par un État membre ou une autorité de contrôle sur le fondement de l'article 26, paragraphe 2, de la directive 95/46/CE demeurent valables jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par ladite autorité de contrôle. Les décisions adoptées par la Commission sur le fondement de l'article 26, paragraphe 4, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par une décision de la Commission adoptée conformément au paragraphe 2 du présent article.

Article 47

Règles d'entreprise contraignantes

1. L'autorité de contrôle compétente approuve des règles d'entreprise contraignantes conformément au mécanisme de contrôle de la cohérence prévu à l'article 63, à condition que:

a) ces règles soient juridiquement contraignantes, et soient mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés;

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

c) elles répondent aux exigences prévues au paragraphe 2.

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

a) la structure et les coordonnées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe et de chacune de leurs entités;

b) les transferts ou l'ensemble des transferts de données, y compris les catégories de données à caractère personnel, le type de traitement et ses finalités, le type de personnes concernées affectées et le nom du ou des pays tiers en question;

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

d) l'application des principes généraux relatifs à la protection des données, notamment la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la qualité des données, la protection des données dès la conception et la protection des données par défaut, la base juridique du traitement, le traitement de catégories particulières de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liés par les règles d'entreprise contraignantes;

e) les droits des personnes concernées à l'égard du traitement et les moyens d'exercer ces droits y compris le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, conformément à l'article 22, le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres conformément à l'article 79 et d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes;

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

g) la manière dont les informations sur les règles d'entreprise contraignantes, notamment en ce qui concerne les éléments mentionnés aux points d), e) et f) du présent paragraphe sont fournies aux personnes concernées, en sus des informations visées aux articles 13 et 14;

h) les missions de tout délégué à la protection des données, désigné conformément à l'article 37, ou de toute autre personne ou entité chargée de la surveillance du respect des règles d'entreprise contraignantes au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, ainsi que le suivi de la formation et le traitement des réclamations;

i) les procédures de réclamation;

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

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

l) le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, notamment en mettant à la disposition de l'autorité de contrôle les résultats des contrôles des mesures visés au point j);

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

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

3. La Commission peut, pour les règles d'entreprise contraignantes au sens du présent article, préciser la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

Article 48

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 ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre.

Article 49

Dérogations pour des situations particulières

1. En l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes:

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

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

c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale;

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

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

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

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

Lorsqu'un transfert ne peut pas être fondé sur une disposition de l'article 45 ou 46, y compris les dispositions relatives aux règles d'entreprise contraignantes, et qu'aucune des dérogations pour des situations particulières visées au premier alinéa du présent paragraphe n'est applicable, un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel. Le responsable du traitement informe l'autorité de contrôle du transfert. Outre qu'il fournit les informations visées aux articles 13 et 14, le responsable du traitement informe la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

2. Un transfert effectué en vertu du paragraphe 1, premier alinéa, point g), ne porte pas sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre. Lorsque le registre est destiné à être consulté par des personnes 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. Les points a), b), et c) du premier alinéa du paragraphe 1 et le deuxième alinéa du paragraphe 1 ne sont pas applicables aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.

4. L'intérêt public visé au paragraphe 1, premier alinéa, point d), est reconnu par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis.

5. En l'absence de décision d'adéquation, le droit de l'Union ou le droit d'un État membre 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. Les États membres notifient de telles dispositions à la Commission.

6. Le responsable du traitement ou le sous-traitant documente, dans les registres visés à l'article 30, l'évaluation ainsi que les garanties appropriées visées au paragraphe 1, deuxième alinéa, du présent article.

Article 50

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

La Commission et les autorités de contrôle prennent, à l'égard des pays tiers et des organisations internationales, les mesures appropriées pour:

a) élaborer des mécanismes de coopération 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

Autorités de contrôle indépendantes

Section 1

Statut d'indépendance

Article 51

Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du présent règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union (ci-après dénommée «autorité de contrôle»).

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

3. Lorsqu'un État membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité et définit le mécanisme permettant de s'assurer du respect, par les autres autorités, des règles relatives au mécanisme de contrôle de la cohérence visé à l'article 63.

4. Chaque État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du présent chapitre, au plus tard, le 25 mai 2018 et, sans tarder, toute modification ultérieure les affectant.

Article 52

Indépendance

1. Chaque autorité de contrôle exerce en toute indépendance les missions et les pouvoirs dont elle est investie conformément au présent règlement.

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

3. Le ou les membres de chaque autorité de contrôle s'abstiennent de tout acte incompatible avec leurs fonctions et, pendant la durée de leur mandat, n'exercent aucune activité professionnelle incompatible, rémunérée ou non.

4. Chaque État membre veille à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsque celle-ci doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité.

5. Chaque État membre veille à ce que chaque autorité de contrôle choisisse et dispose de ses propres agents, qui sont placés sous les ordres exclusifs du ou des membres de l'autorité de contrôle concernée.

6. Chaque État membre veille à ce que chaque autorité de contrôle soit soumise à un contrôle financier qui ne menace pas son indépendance et qu'elle dispose d'un budget annuel public propre, qui peut faire partie du budget global national ou d'une entité fédérée.

Article 53

Conditions générales applicables aux membres de l'autorité de contrôle

1. Les États membres prévoient que chacun des membres de leurs autorités de contrôle est nommé selon une procédure transparente par:

— leur parlement;

— leur gouvernement;

— leur chef d'État; ou

— un organisme indépendant chargé de procéder à la nomination en vertu du le droit de l'État membre

2. Chaque membre a les qualifications, l'expérience et les compétences nécessaires, notamment dans le domaine de la protection des données à caractère personnel, pour l'exercice de ses fonctions et de ses pouvoirs.

3. Les fonctions d'un membre prennent fin à l'échéance de son mandat, en cas de démission ou de mise à la retraite d'office, conformément au droit de l'État membre concerné.

4. Un membre ne peut être démis de ses fonctions que s'il a commis une faute grave ou s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions.

Article 54

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

1. Chaque État membre prévoit, par la loi, tous les éléments suivants:

a) la création de chaque autorité de contrôle;

b) les qualifications et les conditions d'éligibilité requises pour être nommé membre de chaque autorité de contrôle;

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

d) la durée du mandat du ou des membres de chaque autorité de contrôle, qui ne peut être inférieure à quatre ans, sauf pour le premier mandat après le 24 mai 2016, dont une partie peut être d'une durée plus courte lorsque cela est nécessaire pour protéger l'indépendance de l'autorité de contrôle au moyen d'une procédure de nominations échelonnées;

e) le caractère renouvelable ou non du mandat du ou des membres de chaque autorité de contrôle et, si c'est le cas, le nombre de mandats;

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

2. Le ou les membres et les agents de chaque autorité de contrôle sont soumis, conformément au droit de l'Union ou au droit des États membres, au secret professionnel concernant toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs missions ou de leurs pouvoirs, y compris après la fin de leur mandat. Pendant la durée de leur mandat, ce secret professionnel s'applique en particulier au signalement par des personnes physiques de violations du présent règlement.

Section 2

Compétence, missions et pouvoirs

Article 55

Compétence

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

2. Lorsque le traitement est effectué par des autorités publiques ou des organismes privés agissant sur la base de l'article 6, paragraphe 1, point c) ou e), l'autorité de contrôle de l'État membre concerné est compétente. Dans ce cas, l'article 56 n'est pas applicable.

3. Les autorités de contrôle ne sont pas compétentes pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle.

Article 56

Compétence de l'autorité de contrôle chef de file

1. Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60.

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

3. Dans les cas visés au paragraphe 2 du présent article, l'autorité de contrôle informe sans tarder l'autorité de contrôle chef de file de la question. Dans un délai de trois semaines suivant le moment où elle a été informée, l'autorité de contrôle chef de file décide si elle traitera ou non le cas conformément à la procédure prévue à l'article 60, en considérant s'il existe ou non un établissement du responsable du traitement ou du sous-traitant dans l'État membre de l'autorité de contrôle qui l'a informée.

4. Si l'autorité de contrôle chef de file décide de traiter le cas, la procédure prévue à l'article 60 s'applique. L'autorité de contrôle qui a informé l'autorité de contrôle chef de file peut lui soumettre un projet de décision. L'autorité de contrôle chef de file tient le plus grand compte de ce projet lorsqu'elle élabore le projet de décision visé à l'article 60, paragraphe 3.

5. Lorsque l'autorité de contrôle chef de file décide de ne pas traiter le cas, l'autorité de contrôle qui l'a informée le traite conformément aux articles 61 et 62.

6. L'autorité de contrôle chef de file est le seul interlocuteur du responsable du traitement ou du sous-traitant pour le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant.

Article 57

Missions

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

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

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) conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement;

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

e) 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 d'autres États membres;

f) traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association, conformément à l'article 80, examine l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire;

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

h) 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;

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

j) adopte les clauses contractuelles types visées à l'article 28, paragraphe 8, et à l'article 46, paragraphe 2, point d);

k) établit et tient à jour une liste en lien avec l'obligation d'effectuer une analyse d'impact relative à la protection des données en application de l'article 35, paragraphe 4;

l) fournit des conseils sur les opérations de traitement visées à l'article 36, paragraphe 2;

m) encourage l'élaboration de codes de conduite en application de l'article 40, paragraphe 1, rend un avis et approuve les codes de conduite qui fournissent des garanties suffisantes, en application de l'article 40, paragraphe 5;

n) encourage la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données en application de l'article 42, paragraphe 1, et approuve les critères de certification en application de l'article 42, paragraphe 5;

o) procède, le cas échéant, à l'examen périodique des certifications délivrées conformément à l'article 42, paragraphe 7;

p) rédige et publie les critères d'agrément d'un organisme chargé du suivi des codes de conduite en application de l'article 41 et d'un organisme de certification en application de l'article 43;

q) procède à l'agrément d'un organisme chargé du suivi des codes de conduite en application de l'article 41 et d'un organisme de certification en application de l'article 43;

r) autorise les clauses contractuelles et les dispositions visées à l'article 46, paragraphe 3;

s) approuve les règles d'entreprise contraignantes en application de l'article 47;

t) contribue aux activités du comité;

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

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

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

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

4. Lorsque les demandes sont manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif, l'autorité de contrôle peut exiger le paiement de frais raisonnables basés sur les coûts administratifs ou refuser de donner suite à la demande. Il incombe à l'autorité de contrôle de démontrer le caractère manifestement infondé ou excessif de la demande.

Article 58

Pouvoirs

1. Chaque autorité de contrôle dispose de tous les pouvoirs d'enquête suivants:

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

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

c) procéder à un examen des certifications délivrées en application de l'article 42, paragraphe 7;

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

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

f) 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. Chaque autorité de contrôle dispose du pouvoir d'adopter toutes 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) ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement;

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

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

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

g) ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19;

h) retirer une certification ou ordonner à l'organisme de certification de retirer une certification délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites;

i) imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas;

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

3. Chaque autorité de contrôle dispose de tous les pouvoirs d'autorisation et de tous les pouvoirs consultatifs suivants:

a) conseiller le responsable du traitement conformément à la procédure de consultation préalable visée à l'article 36;

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

c) autoriser le traitement visé à l'article 36, paragraphe 5, si le droit de l'État membre exige une telle autorisation préalable;

d) rendre un avis sur les projets de codes de conduite et les approuver en application de l'article 40, paragraphe 5;

e) agréer des organismes de certification en application de l'article 43;

f) délivrer des certifications et approuver des critères de certification conformément à l'article 42, paragraphe 5;

g) adopter les clauses types de protection des données visées à l'article 28, paragraphe 8, et à l'article 46, paragraphe 2, point d);

h) autoriser les clauses contractuelles visées à l'article 46, paragraphe 3, point a);

i) autoriser les arrangements administratifs visés à l'article 46, paragraphe 3, point b);

j) approuver les règles d'entreprise contraignantes en application de l'article 47.

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

5. Chaque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter toute violation du présent règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement.

6. Chaque État membre peut prévoir, par la loi, que son autorité de contrôle dispose de pouvoirs additionnels à ceux visés aux paragraphes 1, 2 et 3. L'exercice de ces pouvoirs n'entrave pas le bon fonctionnement du chapitre VII.

Article 59

Rapports d'activité

Chaque autorité de contrôle établit un rapport annuel sur ses activités, qui peut comprendre une liste des types de violations notifiées et des types de mesures prises conformément à l'article 58, paragraphe 2. Ces rapports sont transmis au parlement national, au gouvernement et à d'autres autorités désignées par le droit de l'État membre. Ils sont mis à la disposition du public, de la Commission et du comité.

CHAPITRE VII

Coopération et cohérence

Section 1

Coopération

Article 60

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

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

2. L'autorité de contrôle chef de file peut demander à tout moment aux autres autorités de contrôle concernées de se prêter mutuellement assistance en application de l'article 61 et peut mener des opérations conjointes en application de l'article 62, en particulier pour effectuer des enquêtes ou contrôler l'application d'une mesure concernant un responsable du traitement ou un sous-traitant établi dans un autre État membre.

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

4. Lorsqu'une des autres autorités de contrôle concernées formule, dans un délai de quatre semaines après avoir été consultée conformément au paragraphe 3 du présent article, une objection pertinente et motivée à l'égard du projet de décision, l'autorité de contrôle chef de file, si elle ne suit pas l'objection pertinente et motivée ou si elle est d'avis que cette objection n'est pas pertinente ou motivée, soumet la question au mécanisme de contrôle de la cohérence visé à l'article 63.

5. Lorsque l'autorité de contrôle chef de file entend suivre l'objection pertinente et motivée formulée, elle soumet aux autres autorités de contrôle concernées un projet de décision révisé en vue d'obtenir leur avis. Ce projet de décision révisé est soumis à la procédure visée au paragraphe 4 dans un délai de deux semaines.

6. Lorsqu'aucune des autres autorités de contrôle concernées n'a formulé d'objection à l'égard du projet de décision soumis par l'autorité de contrôle chef de file dans le délai visé aux paragraphes 4 et 5, l'autorité de contrôle chef de file et les autorités de contrôle concernées sont réputées approuver ce projet de décision et sont liées par lui.

7. L'autorité de contrôle chef de file adopte la décision, la notifie à l'établissement principal ou à l'établissement unique du responsable du traitement ou du sous-traitant, selon le cas, et informe les autres autorités de contrôle concernées et le comité de la décision en question, y compris en communiquant un résumé des faits et motifs pertinents. L'autorité de contrôle auprès de laquelle une réclamation a été introduite informe de la décision l'auteur de la réclamation.

8. Par dérogation au paragraphe 7, lorsqu'une réclamation est refusée ou rejetée, l'autorité de contrôle auprès de laquelle la réclamation a été introduite adopte la décision, la notifie à l'auteur de la réclamation et en informe le responsable du traitement.

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

10. Après avoir été informé de la décision de l'autorité de contrôle chef de file en application des paragraphes 7 et 9, le responsable du traitement ou le sous-traitant prend les mesures nécessaires pour assurer le respect de cette décision en ce qui concerne les activités de traitement menées dans le cadre de tous ses établissements dans l'Union. Le responsable du traitement ou le sous-traitant notifie les mesures prises pour assurer le respect de la décision à l'autorité de contrôle chef de file, qui informe les autres autorités de contrôle concernées.

11. Lorsque, dans des circonstances exceptionnelles, une autorité de contrôle concernée a des raisons de considérer qu'il est urgent d'intervenir pour protéger les intérêts des personnes concernées, la procédure d'urgence visée à l'article 66 s'applique.

12. L'autorité de contrôle chef de file et les autres autorités de contrôle concernées se communiquent par voie électronique et au moyen d'un formulaire type, les informations requises en vertu du présent article.

Article 61

Assistance mutuelle

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

2. Chaque autorité de contrôle prend toutes les mesures appropriées requises pour répondre à une demande d'une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande. De telles mesures peuvent comprendre, notamment, la transmission d'informations utiles sur la conduite d'une enquête.

3. Les demandes d'assistances contiennent toutes les informations nécessaires, notamment la finalité et les motifs de la demande. Les informations échangées ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

4. Une autorité de contrôle requise ne peut refuser de satisfaire à une demande d'assistance, sauf si:

a) elle n'est pas compétente pour traiter l'objet de la demande ou pour prendre les mesures qu'elle est requise d'exécuter; ou

b) satisfaire à la demande constituerait une violation du présent règlement ou du droit de l'Union ou du droit de l'État membre auquel l'autorité de contrôle qui a reçu la demande est soumise.

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

6. En règle générale, les autorités de contrôle requises communiquent par voie électronique et au moyen d'un formulaire type, les informations demandées par d'autres autorités de contrôle.

7. Les autorités de contrôle requises ne perçoivent pas de frais pour toute action qu'elles prennent à la suite d'une demande d'assistance mutuelle. Les autorités de contrôle peuvent convenir de règles concernant l'octroi de dédommagements entre elles pour des dépenses spécifiques résultant de la fourniture d'une assistance mutuelle dans des circonstances exceptionnelles.

8. Lorsqu'une autorité de contrôle ne fournit pas les informations visées au paragraphe 5 du présent article dans un délai d'un mois à compter de la réception de la demande formulée par une autre autorité de contrôle, l'autorité de contrôle requérante peut adopter une mesure provisoire sur le territoire de l'État membre dont elle relève conformément à l'article 55, paragraphe 1. Dans ce cas, les circonstances permettant de considérer qu'il est urgent d'intervenir conformément à l'article 66, paragraphe 1, sont réputées réunies et nécessitent une décision contraignante d'urgence du comité en application de l'article 66, paragraphe 2.

9. La Commission peut, par voie d'actes d'exécution, préciser la forme et les procédures de l'assistance mutuelle visée au présent article, ainsi que les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle et entre les autorités de contrôle et le comité, notamment en ce qui concerne le formulaire type visé au paragraphe 6 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

Article 62

Opérations conjointes des autorités de contrôle

1. Les autorités de contrôle mènent, le cas échéant, des opérations conjointes, y compris en effectuant des enquêtes conjointes et en prenant des mesures répressives conjointes, auxquelles participent des membres ou des agents des autorités de contrôle d'autres États membres.

2. Lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ou si un nombre important de personnes concernées dans plusieurs États membres sont susceptibles d'être sensiblement affectées par des opérations de traitement, une autorité de contrôle de chacun de ces États membres a le droit de participer aux opérations conjointes. L'autorité de contrôle qui est compétente en vertu de l'article 56, paragraphe 1 ou 4, invite l'autorité de contrôle de chacun de ces États membres à prendre part aux opérations conjointes concernées et donne suite sans tarder à toute demande d'une autorité de contrôle souhaitant y participer.

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

4. Lorsque, conformément au paragraphe 1, les agents de l'autorité de contrôle d'origine opèrent dans un autre État membre, l'État membre dont relève l'autorité de contrôle d'accueil assume la responsabilité de leurs actions, y compris la responsabilité des dommages qu'ils causent au cours des opérations dont ils sont chargés, conformément au droit de l'État membre sur le territoire duquel ils opèrent.

5. L'État membre sur le territoire duquel les dommages ont été causés répare ces dommages selon les conditions applicables aux dommages causés par ses propres agents. L'État membre dont relève l'autorité de contrôle d'origine dont les agents ont causé des dommages à des personnes sur le territoire d'un autre État membre rembourse intégralement à cet autre État membre les sommes qu'il a versées aux ayants droit.

6. Sans préjudice de l'exercice de ses droits à l'égard des tiers et sous réserve du paragraphe 5, chaque État membre s'abstient, dans le cas prévu au paragraphe 1, de demander à un autre État membre le remboursement lié aux dommages visés au paragraphe 4.

7. Lorsqu'une opération conjointe est envisagée et qu'une autorité de contrôle ne se conforme pas, dans un délai d'un mois, à l'obligation fixée au paragraphe 2, deuxième phrase, du présent article, les autres autorités de contrôle peuvent adopter une mesure provisoire sur le territoire de l'État membre dont celle-ci relève conformément à l'article 55. Dans ce cas, les circonstances permettant de considérer qu'il est urgent d'intervenir conformément à l'article 66, paragraphe 1, sont présumées être réunies et nécessitent un avis ou une décision contraignante d'urgence du comité en application de l'article 66, paragraphe 2.

Section 2

Cohérence

Article 63

Mécanisme de contrôle de la cohérence

Afin de contribuer à l'application cohérente du présent règlement dans l'ensemble de l'Union, les autorités de contrôle coopèrent entre elles et, le cas échéant, avec la Commission dans le cadre du mécanisme de contrôle de la cohérence établi dans la présente section.

Article 64

Avis du comité

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

a) vise à adopter une liste d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données doit être effectuée en application de l'article 35, paragraphe 4;

b) concerne la question de savoir, en application de l'article 40, paragraphe 7, si un projet de code de conduite ou une modification ou une prorogation d'un code de conduite respecte le présent règlement;

c) vise à approuver les critères d'agrément d'un organisme en application de l'article 41, paragraphe 3, ou d'un organisme de certification en application de l'article 43, paragraphe 3;

d) vise à fixer des clauses types de protection des données visées à l'article 46, paragraphe 2, point d), et à l'article 28, paragraphe 8;

e) vise à autoriser les clauses contractuelles visées à l'article 46, paragraphe 3, point a); ou

f) vise à approuver des règles d'entreprise contraignantes au sens de l'article 47.

2. Toute autorité de contrôle, le président du comité ou la Commission peuvent demander que toute question d'application générale ou produisant des effets dans plusieurs États membres soit examinée par le comité en vue d'obtenir un avis, en particulier lorsqu'une autorité de contrôle compétente ne respecte pas les obligations relatives à l'assistance mutuelle conformément à l'article 61 ou les obligations relatives aux opérations conjointes conformément à l'article 62.

3. Dans les cas visés aux paragraphes 1 et 2, le comité émet un avis sur la question qui lui est soumise, à condition qu'il n'ait pas déjà émis un avis sur la même question. Cet avis est adopté dans un délai de huit semaines à la majorité simple des membres du comité. Ce délai peut être prolongé de six semaines en fonction de la complexité de la question. En ce qui concerne le projet de décision visé au paragraphe 1 transmis aux membres du comité conformément au paragraphe 5, un membre qui n'a pas formulé d'objection dans un délai raisonnable fixé par le président est réputé approuver le projet de décision.

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

5. Le président du comité transmet dans les meilleurs délais par voie électronique:

a) toutes les informations utiles qui lui ont été communiquées aux membres du comité et à la Commission, au moyen d'un formulaire type. Le secrétariat du comité fournit, si nécessaire, les traductions des informations utiles; et

b) l'avis à l'autorité de contrôle visée, selon le cas, aux paragraphes 1 et 2, et à la Commission, et le publie.

6. L'autorité de contrôle compétente n'adopte pas son projet de décision visé au paragraphe 1 lorsque le délai visé au paragraphe 3 court.

7. L'autorité de contrôle visée au paragraphe 1 tient le plus grand compte de l'avis du comité et fait savoir au président du comité par voie électronique au moyen d'un formulaire type, dans un délai de deux semaines suivant la réception de l'avis, si elle maintiendra ou si elle modifiera son projet de décision et, le cas échéant, son projet de décision modifié.

8. Lorsque l'autorité de contrôle concernée informe le président du comité dans le délai visé au paragraphe 7 du présent article qu'elle n'a pas l'intention de suivre, en tout ou en partie, l'avis du comité, en fournissant les motifs pertinents, l'article 65, paragraphe 1, s'applique.

Article 65

Règlement des litiges par le comité

1. En vue d'assurer l'application correcte et cohérente du présent règlement dans les cas d'espèce, le comité adopte une décision contraignante dans les cas suivants:

a) lorsque, dans le cas visé à l'article 60, paragraphe 4, une autorité de contrôle concernée a formulé une objection pertinente et motivée à l'égard d'un projet de décision de l'autorité de contrôle chef de file ou que l'autorité de contrôle chef de file a rejeté cette objection au motif qu'elle n'est pas pertinente ou motivée. La décision contraignante concerne toutes les questions qui font l'objet de l'objection pertinente et motivée, notamment celle de savoir s'il y a violation du présent règlement;

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

c) lorsqu'une autorité de contrôle compétente ne demande pas l'avis du comité dans les cas visés à l'article 64, paragraphe 1, ou qu'elle ne suit pas l'avis du comité émis en vertu de l'article 64. Dans ce cas, toute autorité de contrôle concernée ou la Commission peut saisir le comité de la question.

2. La décision visée au paragraphe 1 est adoptée à la majorité des deux tiers des membres du comité dans un délai d'un mois à compter de la transmission de la question. Ce délai peut être prolongé d'un mois en fonction de la complexité de la question. La décision visée au paragraphe 1, est motivée et est adressée à l'autorité de contrôle chef de file et à toutes les autorités de contrôle concernées et est contraignante à leur égard.

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

4. Les autorités de contrôle concernées n'adoptent pas de décision sur la question soumise au comité en vertu du paragraphe 1 lorsque les délais visés aux paragraphes 2 et 3 courent.

5. Le président du comité notifie, dans les meilleurs délais, la décision visée au paragraphe 1 aux autorités de contrôle concernées. Il en informe la Commission. La décision est publiée sur le site internet du comité sans tarder après que l'autorité de contrôle a notifié la décision finale visée au paragraphe 6.

6. L'autorité de contrôle chef de file ou, selon le cas, l'autorité de contrôle auprès de laquelle la réclamation a été introduite adopte sa décision finale sur la base de la décision visée au paragraphe 1 du présent article, dans les meilleurs délais et au plus tard un mois après que le comité a notifié sa décision. L'autorité de contrôle chef de file ou, selon le cas, l'autorité de contrôle auprès de laquelle la réclamation a été introduite informe le comité de la date à laquelle sa décision finale est notifiée, respectivement, au responsable du traitement ou au sous-traitant et à la personne concernée. La décision finale des autorités de contrôle concernées est adoptée aux conditions de l'article 60, paragraphes 7, 8 et 9. La décision finale fait référence à la décision visée au paragraphe 1 du présent article et précise que celle-ci sera publiée sur le site internet du comité conformément au paragraphe 5 du présent article. La décision visée au paragraphe 1 du présent article est jointe à la décision finale.

Article 66

Procédure d'urgence

1. Dans des circonstances exceptionnelles, lorsqu'une autorité de contrôle concernée considère qu'il est urgent d'intervenir pour protéger les droits et libertés des personnes concernées, elle peut, par dérogation au mécanisme de contrôle de la cohérence visé aux articles 63, 64 et 65 ou à la procédure visée à l'article 60, adopter immédiatement des mesures provisoires visant à produire des effets juridiques sur son propre territoire et ayant une durée de validité déterminée qui n'excède pas trois mois. L'autorité de contrôle communique sans tarder ces mesures et les raisons de leur adoption aux autres autorités de contrôle concernées, au comité et à la Commission.

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

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

4. Par dérogation à l'article 64, paragraphe 3, et à l'article 65, paragraphe 2, l'avis d'urgence ou la décision contraignante d'urgence visés aux paragraphes 2 et 3 du présent article est adopté dans un délai de deux semaines à la majorité simple des membres du comité.

Article 67

Échange d'informations

La Commission peut adopter des actes d'exécution de portée générale afin de définir les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle, et entre ces autorités et le comité, notamment le formulaire type visé à l'article 64.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

Section 3

Comité européen de la protection des données

Article 68

Comité européen de la protection des données

1. Le comité européen de la protection des données (ci-après dénommé «comité») est institué en tant qu'organe de l'Union et possède la personnalité juridique.

2. Le comité est représenté par son président.

3. Le comité se compose du chef d'une autorité de contrôle de chaque État membre et du Contrôleur européen de la protection des données, ou de leurs représentants respectifs.

4. Lorsque, dans un État membre, plusieurs autorités de contrôle sont chargées de surveiller l'application des dispositions du présent règlement, un représentant commun est désigné conformément au droit de cet État membre.

5. La Commission a le droit de participer aux activités et réunions du comité sans droit de vote. La Commission désigne un représentant. Le président du comité informe la Commission des activités du comité.

6. Dans les cas visés à l'article 65, le Contrôleur européen de la protection des données ne dispose de droits de vote qu'à l'égard des décisions concernant des principes et règles applicables aux institutions, organes et organismes de l'Union qui correspondent, en substance, à ceux énoncés dans le présent règlement.

Article 69

Indépendance

1. Le comité exerce les missions et les pouvoirs qui lui sont conférés conformément aux articles 70 et 71 en toute indépendance.

2. Sans préjudice des demandes de la Commission visées à l'article 70, paragraphe 1, point b), et à l'article 70, paragraphe 2, le comité ne sollicite ni n'accepte d'instructions de quiconque dans l'exercice de ses missions et de ses pouvoirs.

Article 70

Missions du comité

1. Le comité veille à l'application cohérente du présent règlement. À cet effet, le comité, de sa propre initiative ou, le cas échéant, à la demande de la Commission, a notamment pour missions:

a) de surveiller et garantir la bonne application du présent règlement dans les cas prévus aux articles 64 et 65, sans préjudice des missions des autorités de contrôle nationales;

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

c) de conseiller la Commission, en ce qui concerne les règles d'entreprise contraignantes, sur la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent;

d) de publier des lignes directrices, des recommandations et des bonnes pratiques sur les procédures de suppression des liens vers des données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication accessibles au public, ainsi que le prévoit l'article 17, paragraphe 2;

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

f) de publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, en vue de préciser davantage les critères et conditions applicables aux décisions fondées sur le profilage en vertu de l'article 22, paragraphe 2;

g) de publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, en vue d'établir les violations de données à caractère personnel, de déterminer les meilleurs délais visés à l'article 33, paragraphes 1 et 2, et de préciser les circonstances particulières dans lesquelles un responsable du traitement ou un sous-traitant est tenu de notifier la violation de données à caractère personnel;

h) de publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe concernant les circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques comme le prévoit l'article 34, paragraphe 1;

i) de publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, aux fins de préciser davantage les critères et exigences applicables aux transferts de données à caractère personnel fondés sur des règles d'entreprise contraignantes appliquées par les responsables du traitement et sur des règles d'entreprise contraignantes appliquées par les sous-traitants et concernant les autres exigences nécessaires pour assurer la protection des données à caractère personnel des personnes concernées visées à l'article 47;

j) de publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, en vue de préciser davantage les critères et exigences applicables aux transferts de données à caractère personnel sur la base de l'article 49, paragraphe 1;

k) d'élaborer, à l'intention des autorités de contrôle, des lignes directrices concernant l'application des mesures visées à l'article 58, paragraphes 1, 2 et 3, ainsi que la fixation des amendes administratives en vertu de l'article 83;

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

m) de publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, en vue d'établir des procédures communes pour le signalement par des personnes physiques de violations du présent règlement en vertu de l'article 54, paragraphe 2;

n) d'encourager l'élaboration de codes de conduite et la mise en place de mécanismes de certification et de labels et de marques en matière de protection des données en vertu des articles 40 et 42;

o) de procéder à l'agrément des organismes de certification et à l'examen périodique de cet agrément en vertu de l'article 43 et de tenir un registre public des organismes agréés en vertu de l'article 43, paragraphe 6, ainsi que des responsables du traitement ou des sous-traitants agréés établis dans des pays tiers en vertu de l'article 42, paragraphe 7;

p) de définir les exigences visées à l'article 43, paragraphe 3, aux fins de l'agrément des organismes de certification prévu à l'article 42;

q) de rendre à la Commission un avis sur les exigences en matière de certification visées à l'article 43, paragraphe 8;

r) de rendre à la Commission un avis sur les icônes visées à l'article 12, paragraphe 7;

s) de rendre à la Commission un avis en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers ou une organisation internationale, y compris concernant l'évaluation visant à déterminer si un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou une organisation internationale n'assurent plus un niveau adéquat de protection. À cette fin, la Commission fournit au comité tous les documents nécessaires, y compris la correspondance avec le gouvernement du pays tiers, en ce qui concerne ledit pays tiers, territoire ou secteur déterminé ou avec l'organisation internationale;

t) d'émettre des avis sur les projets de décisions des autorités de contrôle conformément au mécanisme de contrôle de la cohérence visé à l'article 64, paragraphe 1, sur les questions soumises en vertu de l'article 64, paragraphe 2, et d'émettre des décisions contraignantes en vertu de l'article 65, y compris dans les cas visés à l'article 66;

u) de promouvoir la coopération et l'échange bilatéral et multilatéral effectif d'informations et de bonnes pratiques entre les autorités de contrôle;

v) de promouvoir l'élaboration de programmes de formation conjoints et de faciliter les échanges de personnel entre autorités de contrôle, ainsi que, le cas échéant, avec les autorités de contrôle de pays tiers ou d'organisations internationales;

w) de promouvoir l'échange, avec des autorités de contrôle de la protection des données de tous pays, de connaissances et de documentation sur la législation et les pratiques en matière de protection des données;

x) d'émettre des avis sur les codes de conduite élaborés au niveau de l'Union en application de l'article 40, paragraphe 9; et

y) de tenir un registre électronique, accessible au public, des décisions prises par les autorités de contrôle et les juridictions sur les questions traitées dans le cadre du mécanisme de contrôle de la cohérence.

2. Lorsque la Commission demande conseil au comité, elle peut mentionner un délai, selon l'urgence de la question.

3. Le comité transmet ses avis, lignes directrices, recommandations et bonnes pratiques à la Commission et au comité visé à l'article 93, et les publie.

4. Le comité consulte, le cas échéant, les parties intéressées et leur permet de formuler des observations dans un délai raisonnable. Il met les résultats de la procédure de consultation à la disposition du public, sans préjudice de l'article 76.

Article 71

Rapports

1. Le comité établit un rapport annuel sur la protection des personnes physiques à l'égard du traitement dans l'Union et, s'il y a lieu, dans les pays tiers et les organisations internationales. Le rapport est rendu public et communiqué au Parlement européen, au Conseil et à la Commission.

2. Le rapport annuel présente notamment le bilan de l'application pratique des lignes directrices, recommandations et bonnes pratiques visées à l'article 70, paragraphe 1, point l), ainsi que des décisions contraignantes visées à l'article 65.

Article 72

Procédure

1. Le comité prend ses décisions à la majorité simple de ses membres, sauf disposition contraire du présent règlement.

2. Le comité adopte son règlement intérieur à la majorité des deux tiers de ses membres et détermine ses modalités de fonctionnement.

Article 73

Président

1. Le comité élit son président et deux vice-présidents en son sein à la majorité simple.

2. Le président et les vice-présidents sont élus pour un mandat de cinq ans renouvelable une fois.

Article 74

Missions du président

1. Le président a pour missions:

a) de convoquer les réunions du comité et d'établir l'ordre du jour;

b) de notifier les décisions adoptées par le comité en application de l'article 65 à l'autorité de contrôle chef de file et aux autorités de contrôle concernées;

c) de veiller à l'accomplissement, dans les délais, des missions du comité, notamment en ce qui concerne le mécanisme de contrôle de la cohérence visé à l'article 63.

2. Le comité fixe dans son règlement intérieur la répartition des tâches entre le président et les vice-présidents.

Article 75

Secrétariat

1. Le comité dispose d'un secrétariat, qui est assuré par le Contrôleur européen de la protection des données.

2. Le secrétariat accomplit ses tâches sous l'autorité exclusive du président du comité.

3. Le personnel du Contrôleur européen de la protection des données qui participe à l'exercice des missions que le présent règlement confie au comité est soumis à une structure hiérarchique distincte de celle du personnel qui participe à l'exercice des missions confiées au Contrôleur européen de la protection des données.

4. Le cas échéant, le comité et le Contrôleur européen de la protection des données établissent et publient un protocole d'accord mettant en œuvre le présent article, fixant les modalités de leur coopération et s'appliquant au personnel du Contrôleur européen de la protection des données qui participe à l'exercice des missions que le présent règlement confie au comité.

5. Le secrétariat fournit un soutien analytique, administratif et logistique au comité.

6. Le secrétariat est notamment chargé de:

a) la gestion courante du comité;

b) la communication entre les membres du comité, son président et la Commission;

c) la communication avec d'autres institutions et le public;

d) l'utilisation des voies électroniques pour la communication interne et externe;

e) la traduction des informations utiles;

f) la préparation et le suivi des réunions du comité;

g) la préparation, la rédaction et la publication d'avis, de décisions relatives au règlement des litiges entre autorités de contrôle et d'autres textes adoptés par le comité.

Article 76

Confidentialité

1. Lorsque le comité le juge nécessaire, ses débats sont confidentiels, comme le prévoit son règlement intérieur.

2. L'accès aux documents présentés aux membres du comité, aux experts et aux représentants de tiers est régi par le règlement (CE) nº 1049/2001 du Parlement européen et du Conseil ([1]).

CHAPITRE VIII

Voies de recours, responsabilité et sanctions

Article 77

Droit d'introduire une réclamation auprès d'une autorité de contrôle

1. Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement.

2. L'autorité de contrôle auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article 78.

Article 78

Droit à un recours juridictionnel effectif contre une autorité de contrôle

1. Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne.

2. Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit de former un recours juridictionnel effectif lorsque l'autorité de contrôle qui est compétente en vertu des articles 55 et 56 ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite au titre de l'article 77.

3. Toute action contre une autorité de contrôle est intentée devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie.

4. Dans le cas d'une action intentée contre une décision d'une autorité de contrôle qui a été précédée d'un avis ou d'une décision du comité dans le cadre du mécanisme de contrôle de la cohérence, l'autorité de contrôle transmet l'avis ou la décision en question à la juridiction concernée.

Article 79

Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant

1. Sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement.

2. Toute action contre un responsable du traitement ou un sous-traitant est intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement. Une telle action peut aussi être intentée devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle, sauf si le responsable du traitement ou le sous-traitant est une autorité publique d'un État membre agissant dans l'exercice de ses prérogatives de puissance publique.

([1]) Règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

Article 80

Représentation des personnes concernées

1. 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 d'un État membre, dont les objectifs statutaires sont d'intérêt public et 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 en son nom, exerce en son nom les droits visés aux articles 77, 78 et 79 et exerce en son nom le droit d'obtenir réparation visé à l'article 82 lorsque le droit d'un État membre le prévoit.

2. Les États membres peuvent prévoir que tout organisme, organisation ou association visé au paragraphe 1 du présent article, indépendamment de tout mandat confié par une personne concernée, a, dans l'État membre en question, le droit d'introduire une réclamation auprès de l'autorité de contrôle qui est compétente en vertu de l'article 77, et d'exercer les droits visés aux articles 78 et 79 s'il considère que les droits d'une personne concernée prévus dans le présent règlement ont été violés du fait du traitement.

Article 81

Suspension d'une action

1. Lorsqu'une juridiction compétente d'un État membre est informée qu'une action concernant le même objet a été intentée à l'égard d'un traitement effectué par le même responsable du traitement ou le même sous-traitant et est pendante devant une juridiction d'un autre État membre, elle contacte cette juridiction dans l'autre État membre pour confirmer l'existence d'une telle action.

2. Lorsqu'une action concernant le même objet a été intentée à l'égard d'un traitement effectué par le même responsable du traitement ou le même sous-traitant et est pendante devant une juridiction d'un autre État membre, toute juridiction compétente autre que la juridiction saisie en premier lieu peut suspendre son action.

3. Lorsque cette action est pendante devant des juridictions du premier degré, toute juridiction autre que la juridiction saisie en premier lieu peut également se dessaisir, à la demande de l'une des parties, à condition que la juridiction saisie en premier lieu soit compétente pour connaître des actions en question et que le droit applicable permette leur jonction.

Article 82

Droit à réparation et responsabilité

1. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

2. Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

3. Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

4. Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.

5. Lorsqu'un responsable du traitement ou un sous-traitant a, conformément au paragraphe 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées au paragraphe 2.

6. Les actions judiciaires engagées pour exercer le droit à obtenir réparation sont intentées devant les juridictions compétentes en vertu du droit de l'État membre visé à l'article 79, paragraphe 2.

Article 83

Conditions générales pour imposer des amendes administratives

1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

2. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants:

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi;

b) le fait que la violation a été commise délibérément ou par négligence;

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées;

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32;

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant;

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;

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

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation;

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures;

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42; et

k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

3. Si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du présent règlement, dans le cadre de la même opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave.

4. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu:

a) les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43;

b) les obligations incombant à l'organisme de certification en vertu des articles 42 et 43;

c) les obligations incombant à l'organisme chargé du suivi des codes de conduite en vertu de l'article 41, paragraphe 4.

5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu:

a) les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9;

b) les droits dont bénéficient les personnes concernées en vertu des articles 12 à 22

c) les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale en vertu des articles 44 à 49;

d) toutes les obligations découlant du droit des États membres adoptées en vertu du chapitre IX;

e) le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, ou le fait de ne pas accorder l'accès prévu, en violation de l'article 58, paragraphe 1.

6. Le non-respect d'une injonction émise par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, fait l'objet, conformément au paragraphe 2 du présent article, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

7. Sans préjudice des pouvoirs dont les autorités de contrôle disposent en matière d'adoption de mesures correctrices en vertu de l'article 58, paragraphe 2, chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

8. L'exercice, par l'autorité de contrôle, des pouvoirs que lui confère le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit des États membres, y compris un recours juridictionnel effectif et une procédure régulière.

9. Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, le présent article peut être appliqué de telle sorte que l'amende est déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soit effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle. En tout état de cause, les amendes imposées sont effectives, proportionnées et dissuasives. Les États membres concernés notifient à la Commission les dispositions légales qu'ils adoptent en vertu du présent paragraphe au plus tard le 25 mai 2018 et, sans tarder, toute disposition légale modificative ultérieure ou toute modification ultérieure les concernant.

Article 84

Sanctions

1. Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives.

2. Chaque État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du paragraphe 1 au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant.

CHAPITRE IX

Dispositions relatives à des situations particulières de traitement

Article 85

Traitement et liberté d'expression et d'information

1. Les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire.

2. Dans le cadre du traitement réalisé à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, les États membres prévoient des exemptions ou des dérogations au chapitre II (principes), au chapitre III (droits de la personne concernée), au chapitre IV (responsable du traitement et sous-traitant), au chapitre V (transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales), au chapitre VI (autorités de contrôle indépendantes), au chapitre VII (coopération et cohérence) et au chapitre IX (situations particulières de traitement) si celles-ci sont nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information.

3. Chaque État membre notifie à la Commission les dispositions légales qu'il a adoptées en vertu du paragraphe 2 et, sans tarder, toute disposition légale modificative ultérieure ou toute modification ultérieure les concernant.

Article 86

Traitement et accès du public aux documents officiels

Les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique ou par un organisme public ou un organisme privé pour l'exécution d'une mission d'intérêt public peuvent être communiquées par ladite autorité ou ledit organisme conformément au droit de l'Union ou au droit de l'État membre auquel est soumis l'autorité publique ou l'organisme public, afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel au titre du présent règlement.

Article 87

Traitement du numéro d'identification national

Les États membres peuvent préciser les conditions spécifiques du traitement d'un numéro d'identification national ou de tout autre identifiant d'application générale. Dans ce cas, le numéro d'identification national ou tout autre identifiant d'application générale n'est utilisé que sous réserve des garanties appropriées pour les droits et libertés de la personne concernée adoptées en vertu du présent règlement.

Article 88

Traitement de données dans le cadre des relations de travail

1. Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.

2. Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail.

3. Chaque État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du paragraphe 1 au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant.

Article 89

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

1. 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.

2. 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 ou le droit d'un État membre peut prévoir des dérogations aux droits visés aux articles 15, 16, 18 et 21, sous réserve des conditions et des garanties visées au paragraphe 1 du présent article, 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.

3. Lorsque des données à caractère personnel sont traitées à des fins archivistiques dans l'intérêt public, le droit de l'Union ou le droit d'un État membre peut prévoir des dérogations aux droits visés aux articles 15, 16, 18, 19, 20 et 21, sous réserve des conditions et des garanties visées au paragraphe 1 du présent article, 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. Lorsqu'un traitement visé aux paragraphes 2 et 3 sert dans le même temps une autre finalité, les dérogations sont applicables au seul traitement effectué aux fins visées auxdits paragraphes.

Article 90

Obligations de secret

1. Les États membres peuvent adopter des règles spécifiques afin de définir les pouvoirs des autorités de contrôle visés à l'article 58, paragraphe 1, points e) et f) à l'égard des responsables du traitement ou des sous-traitants qui sont soumis, en vertu du droit de l'Union ou du droit d'un État membre ou de règles arrêtées par les organismes nationaux compétents, à une obligation de secret professionnel ou à d'autres obligations de secret équivalentes, lorsque cela est nécessaire et proportionné pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret. Ces règles ne sont applicables qu'en ce qui concerne les données à caractère personnel que le responsable du traitement ou le sous-traitant a reçues ou a obtenues dans le cadre d'une activité couverte par ladite obligation de secret.

2. Chaque État membre notifie à la Commission les règles qu'il adopte en vertu du paragraphe 1, au plus tard le 25 mai 2018, et, sans tarder, toute modification ultérieure les concernant.

Article 91

Règles existantes des églises et associations religieuses en matière de protection des données

1. Lorsque, dans un État membre, des églises et des associations ou communautés religieuses appliquent, à la date d'entrée en vigueur du présent règlement, un ensemble complet de règles relatives à la protection des personnes physiques à l'égard du traitement, elles peuvent continuer d'appliquer lesdites règles à condition de les mettre en conformité avec le présent règlement.

2. Les églises et les associations religieuses qui appliquent un ensemble complet de règles conformément au paragraphe 1 du présent article sont soumises au contrôle d'une autorité de contrôle indépendante qui peut être spécifique, pour autant qu'elle remplisse les conditions fixées au chapitre VI du présent règlement.

CHAPITRE X

Actes délégués et actes d'exécution

Article 92

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. La délégation de pouvoir visée à l'article 12, paragraphe 8, et à l'article 43, paragraphe 8, est conférée à la Commission pour une durée indéterminée à compter du 24 mai 2016.

3. La délégation de pouvoir visée à l'article 12, paragraphe 8, et à l'article 43, paragraphe 8, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

5. Un acte délégué adopté en vertu de l'article 12, paragraphe 8, et de l'article 43, paragraphe 8, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 93

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 8 du règlement (UE) nº 182/2011, en liaison avec l'article 5, s'applique.

CHAPITRE XI

Dispositions finales

Article 94

Abrogation de la directive 95/46/CE

1. La directive 95/46/CE est abrogée avec effet au 25 mai 2018.

2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE s'entendent comme faites au comité européen de la protection des données institué par le présent règlement.

Article 95

Relation avec la directive 2002/58/CE

Le présent règlement n'impose pas d'obligations supplémentaires aux personnes physiques ou morales quant au traitement dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union en ce qui concerne les aspects pour lesquels elles sont soumises à des obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE.

Article 96

Relation avec les accords conclus antérieurement

Les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales qui ont été conclus par les États membres avant le 24 mai 2016 et qui respectent le droit de l'Union tel qu'il est applicable avant cette date restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation.

Article 97

Rapports de la Commission

1. Au plus tard le 25 mai 2020 et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement. Ces rapports sont publiés.

2. Dans le cadre des évaluations et réexamens visés au paragraphe 1, la Commission examine, en particulier, l'application et le fonctionnement du:

a) chapitre V sur le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, en particulier en ce qui concerne les décisions adoptées en vertu de l'article 45, paragraphe 3 du présent règlement, et des décisions adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE;

b) chapitre VII sur la coopération et la cohérence.

3. Aux fins du paragraphe 1, la Commission peut demander des informations aux États membres et aux autorités de contrôle.

4. Lorsqu'elle procède aux évaluations et réexamens visés aux paragraphes 1 et 2, la Commission tient compte des positions et des conclusions du Parlement européen, du Conseil, et d'autres organismes ou sources pertinents.

5. La Commission soumet, si nécessaire, des propositions appropriées visant à modifier le présent règlement, notamment en tenant compte de l'évolution des technologies de l'information et à la lumière de l'état d'avancement de la société de l'information.

Article 98

Réexamen d'autres actes juridiques de l'Union relatifs à la protection des données

La Commission présente, au besoin, des propositions législatives en vue de modifier d'autres actes juridiques de l'Union relatifs à la protection des données à caractère personnel, afin d'assurer une protection uniforme et cohérente des personnes physiques à l'égard du traitement. Cela concerne en particulier les règles relatives à la protection des personnes physiques à l'égard du traitement par des institutions, organes et organismes de l'Union et à la libre circulation de ces données.

Article 99

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 27 avril 2016.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

Impression: CTIE – Division Imprimés et Fournitures de bureau