COMMISSION EUROPÉENNE

Bruxelles, le 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)

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

{SEC(2012) 72 final}
{SEC(2012) 73 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

Le présent exposé des motifs précise le nouveau cadre juridique envisagé pour la protection des données à caractère personnel dans l'Union européenne, qui est décrit dans la communication COM(2012) 9 final[1]. Ce nouveau cadre juridique se compose de deux propositions législatives:

– une proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), et

– une proposition de directive du Parlement européen et du Conseil 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[2].

Le présent exposé des motifs porte sur la proposition de règlement général sur la protection des données.

La pièce maîtresse de la législation de l'UE en matière de protection des données à caractère personnel, à savoir la directive 95/46/CE[3], avait été adoptée en 1995 avec deux objectifs à l'esprit: protéger le droit fondamental à la protection des données et garantir la libre circulation des données à caractère personnel entre les États membres. Elle a été complétée par la décision-cadre 2008/977/JAI destinée, à titre d'instrument général, au niveau de l'Union, à protéger les données à caractère personnel dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale[4].

La rapide évolution des technologies a créé de nouveaux enjeux pour la protection des données à caractère personnel. Le partage et la collecte de données ont connu une augmentation spectaculaire. Les nouvelles technologies permettent tant aux entreprises privées qu'aux pouvoirs publics d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus de personnes physiques rendent des informations les concernant accessibles à tout un chacun, où qu'il se trouve dans le monde. Les nouvelles technologies ont ainsi transformé l'économie et les rapports sociaux.

Or l'instauration d'un climat de confiance dans l'environnement en ligne est essentielle au développement économique. S'ils n'ont pas totalement confiance, les consommateurs hésiteront à faire des achats en ligne et à recourir à de nouveaux services. Cela risque de

---

1 «Protection de la vie privée dans un monde en réseau – Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle», COM(2012) 9 final.

2 COM(2012) 10 final.

3 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 Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 60, (ci-après «la décision-cadre»).

ralentir l'innovation dans l'utilisation des nouvelles technologies. La protection des données à caractère personnel joue donc un rôle crucial dans la stratégie numérique pour l'Europe[5] et, plus généralement, dans la stratégie Europe 2020[6].

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

Le Conseil européen a invité la Commission à évaluer le fonctionnement des instruments de l'UE relatifs à la protection des données et à présenter, si besoin est, de nouvelles initiatives législatives et non législatives[7]. Dans sa résolution sur le programme de Stockholm, le Parlement européen[8] s'est félicité de la proposition d'un régime complet de protection des données à l'intérieur de l'Union et a, entre autres, plaidé pour une révision de la décision-cadre. Dans son plan d'action mettant en œuvre le programme de Stockholm[9], la Commission insistait sur la nécessité de veiller à ce que le droit fondamental à la protection des données à caractère personnel soit appliqué systématiquement dans le cadre de toutes les politiques européennes.

Dans sa communication intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne»[10], la Commission a conclu que l'UE avait besoin d'une politique plus globale et plus cohérente à l'égard du droit fondamental à la protection des données à caractère personnel.

S'il demeure satisfaisant en ce qui concerne ses objectifs et ses principes, le cadre juridique actuel n'a cependant pas permis d'éviter une fragmentation de la mise en œuvre de la protection des données à caractère personnel dans l'Union, une insécurité juridique et le sentiment, largement répandu dans le public, que des risques importants subsistent, notamment dans l'environnement en ligne[11]. C'est pourquoi il est temps de doter l'Union d'un cadre juridique plus solide et plus cohérent en matière de protection des données, assorti d'une application rigoureuse des règles, afin de permettre à l'économie numérique de se développer sur tout le marché intérieur et aux personnes physiques de maîtriser l'utilisation qui est faite des données les concernant, et de renforcer la sécurité juridique et pratique pour les opérateurs économiques et les pouvoirs publics.

---

5 COM(2010) 245 final.

6 COM(2010) 2020 final.

7 «Le programme de Stockholm – une Europe ouverte et sûre qui sert et protège les citoyens», JO C 115 du 4.5.2010, p. 1.

8 Résolution du Parlement européen du 25 novembre 2009 sur la communication de la Commission au Parlement européen et au Conseil – un espace de liberté, de sécurité et de justice au service des citoyens – programme de Stockholm (P7_TA (2009)0090).

9 COM(2010) 171 final.

10 COM(2010) 609 final.

11 Eurobaromètre spécial (EB) 359, Data Protection and Electronic Identity in the EU (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (en anglais uniquement)..

2. RÉSULTATS DE LA CONSULTATION DES PARTIES INTÉRESSÉES ET DE L'ANALYSE D'IMPACT

La présente initiative fait suite à une vaste consultation des principales parties prenantes sur l'opportunité de réviser le cadre juridique actuel de la protection des données à caractère personnel, qui a duré plus de deux ans et a notamment pris la forme d'une conférence à haut niveau en mai 2009[12] et de deux phases de consultation publique:

– du 9 juillet au 31 décembre 2009, la *consultation sur le cadre juridique applicable au droit fondamental à la protection des données à caractère personnel*. La Commission a reçu 168 réponses, dont 127 provenaient de particuliers, d'organisations et d'associations professionnelles, et 12 de pouvoirs publics[13];

– du 4 novembre 2010 au 15 janvier 2011, la *consultation sur l'approche globale de la Commission en matière de protection des données à caractère personnel dans l'Union européenne*. La Commission a reçu 305 réponses, dont 54 émanaient de citoyens, 31 de pouvoirs publics et 220 d'organismes privés, notamment des associations professionnelles et des organisations non gouvernementales[14].

Des consultations ciblées ont également été menées auprès des principales parties prenantes; des manifestations spécifiques, associant les autorités des États membres et les parties prenantes du secteur privé, ainsi que des organisations de protection des données et de la vie privée, et des associations de consommateurs, ont été organisées en juin et en juillet 2010[15].. En novembre 2010, Mme Viviane Reding, vice-présidente de la Commission européenne, a tenu une table ronde sur la réforme de la protection des données. Le 28 janvier 2011, lors de la Journée de la protection des données, la Commission européenne et le Conseil de l'Europe ont organisé conjointement une conférence à haut niveau afin d'examiner des questions liées à la réforme du cadre juridique de l'UE ainsi que la nécessité d'instaurer des normes communes de protection des données au niveau mondial[16]. Deux conférences sur la protection des données se sont tenues dans le cadre des présidences hongroise et polonaise du Conseil, les 16 et 17 juin 2011 et le 21 septembre 2011 respectivement.

Des ateliers et séminaires spécialisés, portant sur des questions spécifiques, se sont déroulés tout au long de l'année 2011. En janvier, l'ENISA[17] a organisé un atelier sur la notification des violations de données en Europe[18]. En février, la Commission a convoqué un atelier avec les autorités des États membres afin d'examiner des questions liées à la protection des données dans le domaine de la coopération policière et judiciaire en matière pénale, notamment la mise en œuvre de la décision-cadre, et l'Agence des droits fondamentaux a tenu une réunion de consultation des parties prenantes sur «la protection des données et le respect de la vie privée». Une discussion sur des aspects essentiels de la réforme a eu lieu le 13 juillet 2011 avec les autorités nationales chargées de la protection des données. Les citoyens de l'Union

---

12 http://ec.europa.eu/justice/newsroom/data-protection/events/090519_en.htm (en anglais uniquement).

13 Les contributions non confidentielles peuvent être consultées sur le site internet de la Commission: http://ec.europa.eu/justice/newsroom/data-protection/events/090519_en.htm (en anglais uniquement).

14 Les contributions non confidentielles peuvent être consultées sur le site internet de la Commission: http://ec.europa.eu/justice/newsroom/data-protection/events/101104_en.htm (en anglais uniquement).

15 http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm (en anglais uniquement).

16 http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day2011_fr.asp

17 Agence européenne chargée de la sécurité des réseaux et de l'information, qui traite des questions de sécurité relatives aux réseaux de communication et aux systèmes d'information.

18 Voir http://www.enisa.europa.eu/act/it/data-breach-notification

ont été consultés dans le cadre d'une enquête Eurobaromètre qui s'est déroulée aux mois de novembre et décembre 2010[19]. Plusieurs études ont également été entreprises[20]. Le groupe de travail «Article 29»[21] a rendu plusieurs avis et apporté une contribution utile à la Commission[22]. Le contrôleur européen de la protection des données a également rendu un avis exhaustif sur les questions soulevées dans la communication de la Commission de novembre 2010[23].

Par résolution du 6 juillet 2011, le Parlement européen a approuvé un rapport qui appuyait l'approche de la Commission quant à la réforme du cadre législatif régissant la protection des données[24]. Le Conseil de l'Union européenne a adopté, le 24 février 2011, des conclusions dans lesquelles il soutient largement l'intention de la Commission de réformer le cadre de la protection des données et approuve de nombreux éléments de son approche. Le Comité économique et social européen s'est également déclaré favorable à une révision appropriée de la directive 95/46/CE, soutenant l'objectif général de la Commission d'assurer une application plus cohérente des règles européennes en matière de protection des données[25] dans tous les États membres[26].

Au cours des consultations sur l'approche globale, la grande majorité des parties prenantes a reconnu que les principes généraux restaient valables, mais qu'il y avait lieu d'adapter le cadre juridique actuel afin de mieux répondre aux défis posés par la rapide évolution des nouvelles technologies (notamment en ligne) et la mondialisation croissante, tout en préservant la neutralité technologique dudit cadre. La fragmentation de la protection des données à caractère personnel à laquelle nous assistons actuellement dans l'Union a fait l'objet de vives critiques, en particulier de la part des opérateurs économiques, qui réclament une plus grande sécurité juridique et une harmonisation plus poussée des règles en matière de protection des données à caractère personnel. Ils considèrent que la complexité des règles relatives aux transferts internationaux de données à caractère personnel constitue un obstacle

---

19 Eurobaromètre spécial (EB) 359, *Data Protection and Electronic Identity in the EU* (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

20 Voir l'Étude sur les avantages économiques des technologies renforçant la protection de la vie privée, et l'Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques, janvier 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf).

21 Ce groupe de travail a été institué en 1996 (par l'article 29 de la directive). Il s'agit d'un organe consultatif composé de représentants des autorités nationales de contrôle de la protection des données, d'un représentant du contrôleur européen de la protection des données (CEPD) et d'un représentant de la Commission. Pour de plus amples informations sur ses activités, voir: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

22 Voir notamment les avis suivants: sur «L'avenir de la protection de la vie privée» (2009, WP 168); sur les notions de «responsable du traitement» et de «sous-traitant» (1/2010, WP 169); sur la publicité comportementale en ligne (2/2010, WP 171); sur le principe de la responsabilité (3/2010, WP 173); sur le droit applicable (8/2010; WP 179); et sur la définition du consentement (15/2011, WP 187). À la demande de la Commission, il a également adopté trois documents portant respectivement sur les notifications, sur les données sensibles et sur l'application pratique de l'article 28, paragraphe 6, de la directive sur la protection des données. Ces documents peuvent tous être consultés à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm

23 Cet avis est disponible sur le site internet du CEPD: http://www.edps.europa.eu/EDPSWEB

24 Résolution du Parlement européen du 6 juillet 2011 sur une approche globale de la protection des données à caractère personnel dans l'Union européenne (2011/2025(INI), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//FR (rapporteur: le député européen M. Axel Voss (PPE/DE).

25 SEC(2012) 72.

26 CESE 999/2011.

important à leur activité, puisqu'ils ont régulièrement besoin de transférer ce type de données de l'UE vers d'autres parties du monde.

Conformément à sa politique tendant à «mieux légiférer», la Commission a réalisé une analyse d'impact des différentes options possibles. Cette analyse reposait sur trois objectifs, à savoir: renforcer la dimension «marché intérieur» de la protection des données, rendre l'exercice du droit à la protection des données par les personnes physiques plus effectif et instaurer un cadre global et cohérent couvrant tous les domaines de compétence de l'Union, y compris la coopération policière et la coopération judiciaire en matière pénale. Trois options, prévoyant un degré d'intervention variable, ont été évaluées: la première consistait à apporter un minimum de modifications législatives et à recourir à des communications interprétatives et à des mesures de soutien telles que des programmes de financement et des instruments techniques; la deuxième comprenait un ensemble de dispositions législatives répondant à chacun des problèmes mis en évidence dans l'analyse, et la troisième prévoyait la centralisation de la protection des données au niveau de l'UE grâce à l'adoption de règles précises et détaillées pour tous les secteurs et à la création d'une agence européenne chargée de surveiller et de contrôler l'application des dispositions.

Conformément à la méthode établie par la Commission, chaque option a été évaluée, avec l'aide d'un groupe de pilotage interservices, au regard de son efficacité pour atteindre les objectifs fixés, de son impact économique sur les parties prenantes (y compris sur le budget des institutions de l'UE), de son impact social et de son incidence sur les droits fondamentaux. L'impact environnemental n'a pas été examiné. Cette analyse de l'incidence globale des différentes options a permis de dégager l'option privilégiée qui est fondée sur la deuxième option, en y associant quelques éléments des deux autres, et est intégrée dans la présente proposition. D'après l'analyse d'impact, l'option privilégiée devrait permettre, entre autres, de considérablement accroître la sécurité juridique pour les responsables du traitement des données et les citoyens, réduire la charge administrative, harmoniser l'application des règles en matière de protection des données dans l'Union, renforcer l'exercice effectif par les personnes physiques de leur droit à la protection des données les concernant au sein de l'UE et améliorer l'efficacité de la surveillance et du contrôle de l'application des règles en la matière. La mise en œuvre de l'option privilégiée devrait également contribuer à la réalisation de l'objectif de simplification et de réduction de la charge administrative poursuivi par la Commission et des objectifs de la stratégie numérique pour l'Europe, du plan d'action mettant en œuvre le programme de Stockholm et de la stratégie Europe 2020.

Le comité des analyses d'impact a rendu un avis sur le projet d'analyse d'impact le 9 septembre 2011, à la suite de quoi ce dernier a été modifié comme suit:

– les objectifs du cadre juridique actuel (la mesure dans laquelle ils ont été atteints ou ne l'ont pas été) ainsi que ceux de la réforme envisagée ont été précisés;

– des éléments de fait et des explications/précisions ont été ajoutés dans la section relative à la définition des problèmes;

– une section concernant la proportionnalité a été ajoutée;

– tous les calculs et toutes les estimations relatifs à la charge administrative dans le scénario de départ et dans l'option privilégiée ont été entièrement révisés, et le rapport entre le coût des notifications et le coût total de la fragmentation a été clarifié (y compris l'annexe 10);

– les incidences sur les micro, petites et moyennes entreprises, notamment celles de l'obligation de désigner un délégué à la protection des données et de réaliser des analyses d'impact relatives à cette protection ont été précisées.

L'analyse d'impact et son résumé sont publiés avec les propositions.

3. ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

3.1. Base juridique

La présente proposition est fondée sur l'article 16 du TFUE, qui est la nouvelle base juridique, introduite par le traité de Lisbonne, pour l'adoption de règles en matière de protection des données. Cette disposition permet d'adopter des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union. Elle permet également l'adoption de règles relatives à la libre circulation de ces données, y compris les données à caractère personnel traitées par les États membres ou des personnes privées.

Un règlement est considéré comme l'instrument juridique le plus indiqué pour définir le cadre de la protection des données à caractère personnel dans l'Union. Son applicabilité directe, prévue à l'article 288 du TFUE, permettra de réduire la fragmentation juridique et d'apporter une plus grande sécurité juridique, en instaurant un corps harmonisé de règles de base, en améliorant la protection des droits fondamentaux des personnes physiques et en contribuant au bon fonctionnement du marché intérieur.

La référence à l'article 114, paragraphe 1, du TFUE n'est nécessaire qu'aux fins de modification de la directive 2002/58/CE dans la mesure où ladite directive prévoit également la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3.2. Subsidiarité et proportionnalité

Selon le principe de subsidiarité (article 5, paragraphe 3, du TUE), une action au niveau de l'Union est entreprise seulement si, et dans la mesure où, les objectifs envisagés ne peuvent pas être atteints de manière suffisante par les États membres, mais peuvent l'être mieux, en raison des dimensions ou des effets de l'action envisagée, au niveau de l'Union. À la lumière des problèmes décrits ci-dessus, l'analyse de subsidiarité indique la nécessité d'une action au niveau de l'UE pour les raisons suivantes:

– le droit à la protection des données à caractère personnel, consacré à l'article 8 de la charte des droits fondamentaux, exige un niveau de protection des données identique dans l'ensemble de l'Union. L'absence de règles communes dans l'UE risquerait d'entraîner des niveaux de protection différents dans les États membres et, partant, des restrictions sur les flux transfrontières de données à caractère personnel entre les États membres n'appliquant pas les mêmes normes;

– les données à caractère personnel sont transférées de plus en plus rapidement au-delà des frontières nationales, qu'il s'agisse de frontières intérieures ou extérieures. En outre, le contrôle de la bonne application de la législation sur la protection des données pose des problèmes pratiques et il conviendrait d'instaurer une coopération entre les États membres et leurs autorités, organisée au niveau de l'UE, afin d'assurer une application uniforme du

droit de l'Union. L'Union européenne est aussi la mieux placée pour garantir d'une manière efficace et cohérente le même niveau de protection aux personnes physiques, lorsque des données à caractère personnel les concernant sont transférées vers des pays tiers;

– les États membres ne sont pas en mesure de résoudre seuls les problèmes posés par la situation actuelle, en particulier ceux dus à la fragmentation des législations nationales. Aussi y a-t-il précisément lieu de définir un cadre harmonisé et cohérent permettant un transfert aisé des données à caractère personnel au-delà des frontières nationales au sein de l'UE, tout en assurant une protection effective de toutes les personnes physiques dans l'ensemble de l'UE;

– les actions législatives envisagées au niveau de l'UE seront plus efficaces que des actions comparables entreprises au niveau des États membres, compte tenu de la nature et de l'ampleur des problèmes, qui ne se limitent pas à un seul ou à plusieurs États membres.

Le principe de proportionnalité veut que toute intervention soit ciblée et n'excède pas ce qui est nécessaire pour atteindre les objectifs visés. Ce principe a guidé toute l'élaboration de la présente proposition législative, de la détermination et l'évaluation des différentes options jusqu'à sa rédaction.

3.3. Résumé des aspects relatifs aux droits fondamentaux

Le droit à la protection des données à caractère personnel est établi à l'article 8 de la charte et à l'article 16 du TFUE, ainsi qu'à l'article 8 de la CEDH. Ainsi que l'a souligné la Cour de justice de l'Union européenne[27], le droit à la protection des données à caractère personnel n'apparaît pas comme une prérogative absolue, mais doit être pris en considération par rapport à sa fonction dans la société[28]. La protection des données est étroitement liée au respect de la vie privée et familiale, protégé par l'article 7 de la charte. Cela trouve son expression à l'article 1er, paragraphe 1, de la directive 95/46/CE qui dispose que les États membres assurent la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

Les autres droits fondamentaux consacrés dans la charte et susceptibles d'être affectés sont les suivants: la liberté d'expression (article 11 de la charte); la liberté d'entreprise (article 16); le droit de propriété, et notamment la protection de la propriété intellectuelle (article 17, paragraphe 2); l'interdiction de toute discrimination fondée notamment sur la race, les origines ethniques, les caractéristiques génétiques, la religion ou les convictions, les opinions politiques ou toute autre opinion, un handicap ou l'orientation sexuelle (article 21); les droits de l'enfant (article 24); le droit à un niveau élevé de protection de la santé humaine (article 35); le droit d'accès aux documents (article 42); le droit à un recours effectif et à accéder à un tribunal impartial (article 47).

---

27 Cour de justice de l'Union européenne, arrêt du 9 novembre 2010/Arrêt de la Cour de justice de l'Union européenne du 9 novembre 2010 dans les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke GbR et Hartmut Eifert, Rec. 2010, p. I-0000.

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

3.4. Explication détaillée de la proposition

3.4.1. CHAPITRE I - DISPOSITIONS GÉNÉRALES

L'article 1er définit l'objet du règlement et, comme l'article 1er de la directive 95/46/CE, les deux objectifs poursuivis.

L'article 2 délimite le champ d'application matériel du règlement.

L'article 3 délimite le champ d'application territorial du règlement.

L'article 4 définit des termes employés dans le règlement. Certaines définitions sont reprises de la directive 95/46/CE, tandis que d'autres sont modifiées ou complétées par des éléments supplémentaires, ou sont nouvelles (la «violation de données à caractère personnel» dont la définition est fondée sur l'article 2, point h), de la directive 2002/58/CE[29] («vie privée et communications électroniques») telle que modifiée par la directive 2009/136/CE[30], les «données génétiques», les «données biométriques», les «données concernant la santé», l'«établissement principal», le «représentant», l'«entreprise», le «groupe d'entreprises», les «règles d'entreprise contraignantes», l'«enfant» dont la définition est fondée sur la convention des Nations unies relative aux droits de l'enfant[31], et l'«autorité de contrôle»).

Dans la définition du consentement, le qualificatif «explicite» est ajouté à la liste des critères afin d'éviter tout parallélisme prêtant à confusion avec le consentement «indubitable» et de disposer d'une définition unique et cohérente du consentement, garantissant que la personne concernée donne son consentement en toute connaissance de cause.

3.4.2. CHAPITRE II - PRINCIPES

L'article 5 énonce les principes relatifs au traitement des données à caractère personnel, qui correspondent à ceux de l'article 6 de la directive 95/46/CE. Des éléments nouveaux ont été ajoutés, tels que le principe de transparence, des éclaircissements concernant le principe de minimisation des données et l'instauration d'une responsabilité globale du responsable du traitement.

L'article 6 définit, sur la base de l'article 7 de la directive 95/46/CE, les critères de licéité du traitement, qui sont précisés en ce qui concerne la mise en balance des intérêts, et le respect des obligations légales et de l'intérêt général.

L'article 7 précise les conditions auxquelles le consentement peut valablement fonder un traitement licite.

---

29 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.

30 Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, texte présentant de l'intérêt pour l'EEE; JO L 337 du 18.12.2009, p. 11.

31 Adoptée et ouverte à la signature, ratification et adhésion par la résolution 44/25 de l'Assemblée générale des Nations unies du 20 novembre 1989.

L'article 8 fixe d'autres conditions de licéité pour le traitement des données à caractère personnel relatives aux enfants, en ce qui concerne les services de la société de l'information qui sont directement proposés à ces derniers.

L'article 9, qui s'inspire de l'article 8 de la directive 95/46/CE, prévoit une interdiction générale des traitements portant sur des catégories particulières de données à caractère personnel, et les exceptions à cette règle générale.

L'article 10 précise que le responsable du traitement n'est pas tenu d'obtenir des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter une disposition du présent règlement.

3.4.3. CHAPITRE III - DROITS DE LA PERSONNE CONCERNÉE

3.4.3.1. Section 1 – Transparence et modalités

L'article 11 introduit l'obligation, pour les responsables du traitement, de fournir des informations transparentes, facilement accessibles et intelligibles, qui s'inspire notamment de la résolution de Madrid relative à des normes internationales en matière de protection des données à caractère personnel et de la vie privée[32].

L'article 12 oblige le responsable du traitement à prévoir des procédures et des mécanismes permettant à la personne concernée d'exercer ses droits, notamment les moyens d'effectuer une demande par voie électronique, la fixation d'un délai de réponse à la demande de la personne concernée et la motivation des refus.

L'article 13 prévoit des droits en faveur des destinataires inspirés de l'article 12, point c), de la directive 95/46/CE et étendus à tous les destinataires, y compris les responsables conjoints du traitement et les sous-traitants.

3.4.3.2. Section 2 - Information et accès aux données

L'article 14 précise les informations que le responsable du traitement est tenu de fournir à la personne concernée et en ajoute par rapport aux articles 10 et 11 de la directive 95/46/CE, notamment la durée de conservation, le droit d'introduire une réclamation, les transferts internationaux et la source des données. Il reprend également les dérogations prévues dans la directive 95/46/CE, par exemple l'absence d'obligation d'information si la législation prévoit expressément l'enregistrement ou la communication des données. Cela pourrait, par exemple, s'appliquer aux procédures engagées par une autorité de concurrence, une administration fiscale ou douanière, ou un service chargé des questions de sécurité sociale.

L'article 15 confère à la personne concernée un droit d'accès aux données à caractère personnel la concernant, tout comme le faisait l'article 12, point a), de la directive 95/46/CE, en y ajoutant de nouveaux éléments tels que l'obligation d'informer les personnes concernées de la durée de conservation, de leur droit à rectification et à l'effacement et de leur droit de réclamation.

---

[32] Adoptée, le 5 novembre 2009, par la conférence internationale des commissaires à la protection des données et de la vie privée. Cf. également l'article 13, paragraphe 3, de la proposition de règlement relatif à un droit commun européen de la vente [COM(2011) 635 final].

3.4.3.3. Section 3 – Rectification et effacement

L'article 16 confère à la personne concernée un droit à rectification, sur la base de l'article 12, point b), de la directive 95/46/CE.

L'article 17 lui confère, quant à lui, un droit à l'oubli numérique et à l'effacement. Il développe et précise le droit d'effacement prévu à l'article 12, point b), de la directive 95/46/CE et fixe les conditions du droit à l'oubli numérique, notamment l'obligation qui est faite au responsable du traitement ayant rendu publiques des données à caractère personnel d'informer les tiers de la demande de la personne concernée d'effacer tout lien vers ces données ou les copies ou reproductions qui en ont été faites. Il intègre aussi le droit de limiter le traitement dans certains cas, en évitant le terme équivoque de «verrouillage».

L'article 18 confère à la personne concernée un nouveau droit, le droit à la portabilité des données, c'est-à-dire celui de transmettre des données d'un système de traitement automatisé à un autre, sans que le responsable du traitement ne puisse y faire obstacle. À titre de condition préalable et pour améliorer l'accès des personnes physiques aux données à caractère personnel les concernant, il prévoit le droit d'obtenir ces données du responsable du traitement dans un format électronique structuré et couramment utilisé.

3.4.3.4. Section 4 — Droit d'opposition et profilage

L'article 19 confère à la personne concernée un droit d'opposition. Il est fondé sur l'article 14 de la directive 95/46/CE, auquel il apporte quelques modifications, notamment en ce qui concerne la charge de la preuve et son application au marketing direct.

L'article 20 porte sur le droit de la personne concernée de ne pas être soumise à une mesure fondée sur le profilage. Il est inspiré de l'article 15, paragraphe 1, de la directive 95/46 relatif aux décisions individuelles automatisées, qu'il complète et assortit de garanties supplémentaires, et tient compte de la recommandation du Conseil de l'Europe concernant le profilage[33].

3.4.3.5. Section 5 – Limitations

L'article 21 précise dans quelle mesure l'Union ou les États membres peuvent maintenir ou introduire des limitations aux principes énoncés à l'article 5 et aux droits de la personne concernée prévus aux articles 11 à 20 et à l'article 32. Cette disposition repose sur l'article 13 de la directive 95/46/CE et sur les exigences découlant de la charte des droits fondamentaux et de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telles qu'elles ont été interprétées par la Cour de justice de l'Union européenne et par la Cour européenne des droits de l'homme.

3.4.4. CHAPITRE IV - RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT

3.4.4.1. Section 1 — Obligations générales

L'article 22 tient compte du débat sur un «principe de responsabilité» et décrit en détail les obligations incombant au responsable du traitement pour se conformer au présent règlement et

[33] CM/Rec (2010) 13.

en apporter la preuve, notamment par l'adoption de règles internes et de mécanismes à cet effet.

L'article 23 définit les obligations du responsable du traitement qui découlent des principes de protection des données dès la conception et de protection des données par défaut.

L'article 24 relatif aux responsables conjoints du traitement précise les responsabilités de ces derniers en ce qui concerne leurs relations internes et à l'égard de la personne concernée.

L'article 25 oblige, dans certaines circonstances, les responsables du traitement qui ne sont pas établis dans l'Union à y désigner un représentant, lorsque le règlement s'applique à leurs activités de traitement.

L'article 26 précise la fonction de sous-traitant et les obligations qui y sont attachées. Il est en partie fondé sur l'article 17, paragraphe 2, de la directive 95/46/CE, auquel il ajoute de nouveaux éléments, notamment le fait qu'un sous-traitant qui traite des données d'une autre manière que celle prévue dans les instructions du responsable du traitement doit être considéré comme responsable conjoint du traitement.

L'article 27 relatif au traitement effectué sous l'autorité du responsable du traitement et du sous-traitant est fondé sur l'article 16 de la directive 95/46/CE.

L'article 28 introduit l'obligation, pour les responsables du traitement et les sous-traitants, de conserver une trace documentaire des opérations de traitement sous leur responsabilité, au lieu de la notification générale à l'autorité de contrôle exigée par l'article 18, paragraphe 1, et l'article 19 de la directive 95/46/CE.

L'article 29 précise les obligations qui incombent au responsable du traitement et au sous-traitant dans le cadre de leur coopération avec l'autorité de contrôle.

3.4.4.2. Section 2 – Sécurité des données

L'article 30 oblige le responsable du traitement et le sous-traitant à mettre en œuvre les mesures appropriées pour assurer la sécurité du traitement. Fondé sur l'article 17, paragraphe 1, de la directive 95/46/CE, il étend cette obligation aux sous-traitants, indépendamment du contrat conclu avec le responsable du traitement.

Les articles 31 et 32 introduisent une obligation de notification des violations de données à caractère personnel, inspirée de la notification des violations de données à caractère personnel prévue à l'article 4, paragraphe 3, de la directive 2002/58/CE («vie privée et communications électroniques»).

3.4.4.3. Section 3 – Évaluation de la protection des données et autorisation préalable

L'article 33 introduit l'obligation, pour les responsables du traitement et les sous-traitants, d'effectuer une analyse d'impact relative à la protection des données préalablement aux traitements présentant des risques.

L'article 34, qui développe la notion de contrôles préalables définie à l'article 20 de la directive 95/46/CE, concerne les cas dans lesquels l'autorisation et la consultation de l'autorité de contrôle sont obligatoires avant le traitement.

3.4.4.4. Section 4 – Délégué à la protection des données

L'article 35 introduit l'obligation de désigner un délégué à la protection des données pour le secteur public et, dans le secteur privé, pour les grandes entreprises, ou lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des traitements qui exigent un suivi régulier et systématique. Cette disposition s'inscrit dans la continuité de l'article 18, paragraphe 2, de la directive 95/46/CE, qui prévoyait la possibilité pour les États membres d'introduire une telle obligation à la place de l'obligation de notification générale.

L'article 36 définit la fonction du délégué à la protection des données.

L'article 37 prévoit les principales tâches du délégué à la protection des données.

3.4.4.5. Section 5 – Codes de conduite et certification

L'article 38 porte sur les codes de conduite. Il développe la notion figurant à l'article 27, paragraphe 1, de la directive 95/46/CE, précise le contenu des codes et des procédures, et habilite la Commission à se prononcer sur l'applicabilité générale des codes de conduite.

L'article 39 introduit la possibilité de mettre en place des mécanismes de certification ainsi que des marques et labels en matière de protection des données.

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

L'article 40 pose le principe général selon lequel le respect des obligations énoncées dans ce chapitre est obligatoire pour tout transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris les transferts ultérieurs.

L'article 41 définit, sur la base de l'article 25 de la directive 95/46/CE, les critères, conditions et procédures d'adoption d'une décision de la Commission constatant un niveau de protection adéquat. Les critères devant être pris en compte par la Commission aux fins de l'appréciation d'un niveau de protection adéquat ou non incluent expressément l'État de droit, l'existence d'un droit de recours judiciaire et un contrôle indépendant. Cet article confirme désormais explicitement la faculté de la Commission d'apprécier le niveau de protection assuré par un territoire ou un secteur de traitement des données à l'intérieur d'un pays tiers.

L'article 42 subordonne les transferts vers des pays tiers pour lesquels la Commission n'a pas adopté de décision constatant un niveau de protection adéquat, à la présentation de garanties appropriées, notamment des clauses types de protection des données, des règles d'entreprise contraignantes et des clauses contractuelles. La possibilité d'utiliser des clauses types de protection des données de la Commission est tirée de l'article 26, paragraphe 4, de la directive 95/46/CE. Une nouveauté réside dans le fait que ces clauses types de protection des données peuvent désormais être également adoptées par une autorité de contrôle et être déclarées, par la Commission, généralement applicables. Les règles d'entreprise contraignantes sont à présent expressément mentionnées dans le texte juridique. L'option des clauses contractuelles offre une certaine souplesse au responsable du traitement ou au sous-traitant, mais est subordonnée à l'autorisation préalable d'une autorité de contrôle.

L'article 43 décrit plus en détail les conditions applicables aux transferts encadrés par des règles d'entreprise contraignantes, sur la base des pratiques et des exigences actuelles des autorités de contrôle.

L'article 44 définit et précise les dérogations autorisées pour les transferts de données, sur la base des dispositions existantes de l'article 26 de la directive 95/46/CE. Cette disposition s'applique en particulier aux transferts de données qui sont nécessaires pour des motifs importants d'intérêt général, par exemple en cas de transfert international de données entre autorités de la concurrence, administrations fiscales ou douanières, ou entre services chargés des questions de sécurité sociale ou de la gestion des activités de pêche. En outre, un transfert de données peut, dans certaines circonstances, être justifié par un intérêt légitime du responsable du traitement ou du sous-traitant, mais seulement après évaluation et justification des circonstances de cette opération de transfert.

L'article 45 prévoit expressément l'élaboration de mécanismes de coopération internationaux dans le domaine de la protection des données à caractère personnel, entre la Commission et les autorités de contrôle de pays tiers, notamment ceux qui sont réputés assurer un niveau de protection adéquat, compte tenu de la recommandation de l'Organisation de coopération et de développement économiques (OCDE) du 12 juin 2007 relative à la coopération transfrontière dans l'application des législations protégeant la vie privée.

3.4.6. CHAPITRE VI – AUTORITÉS DE CONTRÔLE INDÉPENDANTES

3.4.6.1. Section 1 – Statut d'indépendance

L'article 46 fait obligation aux États membres de mettre en place une ou plusieurs autorités de contrôle, ainsi que le requérait l'article 28, paragraphe 1, de la directive 95/46/CE, et d'élargir la mission de celles-ci à la coopération entre elles et avec la Commission.

L'article 47 clarifie les conditions garantissant l'indépendance des autorités de contrôle, en application de la jurisprudence de la Cour de justice de l'Union européenne[34], et en s'inspirant également de l'article 44 du règlement (CE) n° 45/2001[35].

L'article 48 énonce les conditions générales applicables aux membres de l'autorité de contrôle, en application de la jurisprudence en la matière[36], et en s'inspirant également de l'article 42, paragraphes 2 à 6, du règlement (CE) n° 45/2001.

L'article 49 définit les règles encadrant la mise en place de l'autorité de contrôle, que les États membres devront fixer par voie législative.

Fondé sur l'article 28, paragraphe 7, de la directive 95/46/CE, l'article 50 impose le secret professionnel aux membres et au personnel de l'autorité de contrôle.

---

34 Arrêt de la Cour de justice de l'Union européenne du 9 mars 2010 dans l'affaire C-518/07, Commission/Allemagne, Rec. 2010, p. I-1885.

35 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.

36 Op. cit., note de bas de page n° 34.

3.4.6.2. Section 2 – Fonctions et pouvoirs

L'article 51 définit la compétence des autorités de contrôle. La règle générale, reposant sur l'article 28, paragraphe 6, de la directive 95/46/CE (compétence sur le territoire l'État membre dont l'autorité relève) est complétée par une nouvelle compétence, celle d'autorité chef de file lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres, afin d'assurer une application uniforme («guichet unique»). Lorsqu'elles agissent dans le cadre de leur fonction juridictionnelle, les juridictions sont dispensées de se soumettre à la surveillance de l'autorité de contrôle, mais pas d'appliquer les règles matérielles relatives à la protection de données.

L'article 52 définit les fonctions de l'autorité de contrôle, consistant notamment à recevoir et à examiner les réclamations, et à sensibiliser le public aux risques, règles, garanties et droits existants.

L'article 53 énonce les pouvoirs de l'autorité de contrôle, en s'appuyant en partie sur l'article 28, paragraphe 3, de la directive 95/46/CE et sur l'article 47 du règlement (CE) n° 45/2001, et en y ajoutant quelques éléments nouveaux, dont le pouvoir de sanctionner les infractions administratives.

L'article 54 fait obligation aux autorités de contrôle d'établir des rapports d'activité annuels, ainsi que le requérait l'article 28, paragraphe 5, de la directive 95/46/CE.

3.4.7. CHAPITRE VII - COOPÉRATION ET COHÉRENCE

3.4.7.1. Section 1 – Coopération

L'article 55 instaure des règles explicites en matière d'assistance mutuelle obligatoire et prévoit notamment les conséquences en cas de refus de se conformer à la demande d'une autre autorité de contrôle, sur la base de l'article 28, paragraphe 6, deuxième alinéa, de la directive 95/46/CE.

L'article 56 établit des règles applicables aux opérations conjointes, s'inspirant de l'article 17 de la décision 2008/615/JAI du Conseil[37], y compris le droit conféré aux autorités de contrôle de participer à ces opérations.

3.4.7.2. Section 2 – Cohérence

L'article 57 met en place un mécanisme de contrôle de la cohérence, en vue d'assurer une application uniforme des règles lorsqu'il s'agit de traitements qui peuvent viser des personnes concernées dans plusieurs États membres.

L'article 58 définit les procédures et conditions à respecter pour demander l'avis du comité européen de la protection des données.

L'article 59 concerne les avis de la Commission relatifs aux questions examinées dans le cadre du mécanisme de contrôle de la cohérence, qui peuvent soit confirmer l'avis du comité

[37] Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JO L 210 du 6.8.2008, p. 1.

européen de la protection des données soit diverger de cet avis, et ceux relatifs aux projets de mesure transmis par l'autorité de contrôle. Lorsque la question a été soulevée par le comité européen de la protection des données en vertu de l'article 58, paragraphe 3, la Commission est susceptible d'exercer son pouvoir discrétionnaire et, au besoin, de rendre un avis.

L'article 60 concerne la décision que la Commission peut prendre pour contraindre une autorité compétente à suspendre son projet de mesure lorsque cela est nécessaire pour garantir l'application correcte du présent règlement.

L'article 61 prévoit la possibilité d'adopter des mesures provisoires, selon une procédure d'urgence.

L'article 62 définit les conditions relatives à l'adoption d'actes d'exécution de la Commission dans le cadre du mécanisme de contrôle de la cohérence.

L'article 63 prévoit l'obligation d'exécuter la mesure prévue par une autorité de contrôle dans tous les États membres concernés, et précise que l'application du mécanisme de contrôle de la cohérence est une condition préalable à la validité juridique et à l'exécution de la mesure concernée.

3.4.7.3. Section 3 – Comité européen de la protection des données

L'article 64 institue le comité européen de la protection des données, composé des directeurs des autorités de contrôle de tous les États membres et du contrôleur européen à la protection des données. Le comité européen de la protection des données remplace le groupe de protection des personnes à l'égard du traitement des données à caractère personnel créé par l'article 29 de la directive 95/46/CE. L'article 65 précise que la Commission n'est pas membre de ce comité, mais a le droit de participer à ses activités et de s'y faire représenter.

L'article 65 souligne et explicite l'indépendance du comité européen de la protection des données.

L'article 66 décrit les missions du comité européen de la protection des données, sur la base de l'article 30, paragraphe 1, de la directive 95/46/CE, et prévoit des éléments supplémentaires, pour tenir compte de l'élargissement du domaine d'activités de ce comité, tant au sein qu'à l'extérieur de l'Union. Pour être en mesure de réagir à des situations d'urgence, la Commission a la possibilité de demander audit comité de formuler un avis dans un délai donné.

L'article 67 fait obligation au comité européen de la protection des données de présenter un rapport annuel sur ses activités, sur la base de l'article 30, paragraphe 6, de la directive 95/46/CE.

L'article 68 définit les procédures décisionnelles du comité européen de la protection des données, y compris l'obligation d'adopter un règlement intérieur devant également déterminer ses modalités de fonctionnement.

L'article 69 contient des dispositions relatives au président et aux vice-présidents du comité européen de la protection des données.

L'article 70 définit les missions du président.

L'article 71 prévoit que le secrétariat du comité européen de la protection des données est assuré par le contrôleur européen de la protection des données et il précise les missions de ce secrétariat.

L'article 72 définit les règles de confidentialité.

3.4.8. CHAPITRE III – VOIES DE RECOURS, RESPONSABILITÉ ET SANCTIONS

L'article 73 prévoit le droit de toute personne concernée de déposer une réclamation auprès d'une autorité de contrôle, sur la base de l'article 28, paragraphe 4, de la directive 95/46/CE. Il précise également les organismes, organisations ou associations habilités à déposer une réclamation au nom de la personne concernée ou, en cas de violation de données à caractère personnel, indépendamment de toute réclamation introduite par une personne concernée.

L'article 74 concerne le droit de former un recours juridictionnel contre une autorité de contrôle. Il s'appuie sur la disposition générale figurant à l'article 28, paragraphe 3 de la directive 95/46/CE et prévoit, en particulier, un recours juridictionnel pour contraindre une autorité de contrôle à donner suite à une réclamation, tout en clarifiant la compétence des juridictions de l'État membre où l'autorité de contrôle est établie. Il prévoit également la possibilité que l'autorité de contrôle de l'État membre de résidence de la personne concernée intente, au nom de cette dernière, une action devant les juridictions d'un autre État membre dans lequel l'autorité de contrôle compétente est établie.

L'article 75 concerne le droit de former un recours juridictionnel contre un responsable du traitement ou un sous-traitant, s'appuyant sur l'article 22 de la directive 95/46/CE, et offre le choix de saisir une juridiction dans l'État membre où le défendeur est établi ou dans l'État membre de résidence de la personne concernée. Lorsqu'une procédure portant sur la même question est pendante dans le cadre du mécanisme de contrôle de la cohérence, la juridiction peut suspendre sa procédure/surseoir à statuer, sauf en cas d'urgence.

L'article 76 fixe des règles communes pour les procédures juridictionnelles, y compris le droit conféré à des organismes, organisations ou associations de représenter les personnes concernées devant les tribunaux, le droit des autorités de contrôle d'ester en justice et l'obligation d'informer les juridictions de l'existence d'une procédure parallèle dans un autre État membre, et la possibilité offerte aux juridictions nationales de suspendre la procédure en pareil cas[38]. Les États membres sont tenus de veiller à ce que les actions en justice aboutissent rapidement[39].

L'article 77 traite du droit à réparation et de la responsabilité. Il s'appuie sur l'article 23 de la directive 95/46/CE, étend ce droit aux dommages causés par les sous-traitants et clarifie la responsabilité des responsables conjoints du traitement et des sous-traitants.

---

[38] Sur le fondement de l'article 5, paragraphe 1, de la décision-cadre 2009/948/JAI du Conseil du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales, JO L 328 du 15.12.2009, p. 42; et de l'article 13, paragraphe 1, du règlement (CE) n° 1/2003 du Conseil du 16 décembre 2002 relatif à la mise en œuvre des règles de concurrence prévues aux articles 81 et 82 du traité, JO L 1 du 4.1.2003, p. 1.

[39] Sur le fondement de l'article 18, paragraphe 1, de la 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.

L'article 78 oblige les États membres à définir les sanctions pénales applicables aux infractions aux dispositions du règlement et à veiller à leur application.

L'article 79 impose à chaque autorité de contrôle de sanctionner les infractions administratives énumérées dans cette disposition, par des amendes plafonnées à un certain montant, en fonction des circonstances propres à chaque cas.

3.4.9. CHAPITRE IX - DISPOSITIONS RELATIVES À DES SITUATIONS PARTICULIÈRES DE TRAITEMENT DES DONNÉES

L'article 80 fait obligation aux États membres de prévoir des exemptions et des dérogations à certaines dispositions du règlement lorsqu'elles sont nécessaires pour concilier le droit à la protection des données à caractère personnel avec le droit à la liberté d'expression. Il se fonde sur l'article 9 de la directive 95/46/CE tel qu'il a été interprété par la Cour de justice de l'UE[40].

L'article 81 oblige les États membres à prévoir, outre les conditions applicables à des catégories particulières de données, des garanties spécifiques en cas de traitement de données concernant la santé.

L'article 82 habilite les États membres à adopter, par voie législative, des règles spécifiques pour le traitement des données à caractère personnel dans le secteur de l'emploi.

L'article 83 définit des conditions spécifiques pour le traitement de données à caractère personnel à des fins historiques, statistiques et de recherche scientifique.

L'article 84 habilite les États membres à adopter des règles spécifiques régissant l'accès des autorités de contrôle aux données à caractère personnel et aux locaux, lorsque les responsables du traitement sont soumis à des obligations de confidentialité.

L'article 85 autorise les églises, en vertu de l'article 17 du traité sur le fonctionnement de l'Union européenne, à continuer à appliquer un ensemble complet de règles de protection des données, à condition de les mettre en conformité avec le présent règlement.

3.4.10. CHAPITRE X - ACTES DÉLÉGUÉS ET ACTES D'EXÉCUTION

L'article 86 contient les dispositions types applicables à l'exercice de la délégation, conformément à l'article 290 du TFUE. Ce dernier autorise le législateur à déléguer à la Commission le pouvoir d'adopter des actes non législatifs de portée générale qui complètent ou modifient certains éléments non essentiels d'un acte législatif (actes quasi législatifs).

L'article 87 contient la disposition relative à la procédure de comité nécessaire pour conférer des compétences d'exécution à la Commission, dans les cas où, conformément à l'article 291 du TFUE, des conditions uniformes d'exécution d'actes juridiquement contraignants de l'Union sont nécessaires. La procédure d'examen s'applique.

---

[40] Voir, par exemple, pour l'interprétation de la Cour de justice de l'UE, l'arrêt du 16 décembre 2008 dans l'affaire C-73/07, Satakunnan Markkinapörssi et Satamedia, Rec. 2008, p. I-9831.

3.4.11. CHAPITRE XI - DISPOSITIONS FINALES

L'article 88 abroge la directive 95/46/CE.

L'article 89 clarifie la relation avec la directive 2002/58/CE («vie privée et communications électroniques») et modifie celle-ci.

L'article 90 fait obligation à la Commission d'évaluer le règlement et de présenter des rapports à ce sujet.

L'article 91 fixe la date d'entrée en vigueur du règlement et définit une période transitoire en ce qui concerne la date de son application.

4. INCIDENCE BUDGÉTAIRE

Les incidences budgétaires spécifiques de la proposition concernent les missions dévolues au contrôleur européen de la protection des données, comme il est indiqué dans la fiche financière législative jointe à la présente proposition. Ces incidences nécessitent une reprogrammation de la rubrique 5 du cadre financier.

La proposition n'a pas d'incidence sur les dépenses de fonctionnement.

La fiche financière législative accompagnant la présente proposition de règlement couvre les incidences budgétaires du règlement lui-même et celles de la directive sur la protection des données dans le domaine de la police et de la justice.

2012/0011 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)

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

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16, paragraphe 2, et son article 114, paragraphe 1,

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[41],

après consultation du contrôleur européen de la protection des données[42],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

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

(2) Le traitement des données à caractère personnel est au service de l'homme; les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données les concernant devraient donc, quelle que soit la nationalité ou la résidence de ces personnes, respecter leurs libertés et leurs droits fondamentaux, notamment le droit à la protection des données à caractère personnel. Le traitement des données devrait contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation

41 JO C du , p. .
42 JO C du , p. .

et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes.

(3) La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[43] vise à harmoniser la protection des libertés et des droits fondamentaux des personnes physiques en ce qui concerne les activités de traitement de données et à garantir la libre circulation des données à caractère personnel entre les États membres.

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

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

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

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

[43] JO L 281 du 23.11.1995, p. 31.

fausser la concurrence et empêcher les autorités de s'acquitter des obligations qui leur incombent en vertu du droit de l'Union. Ces écarts de niveau de protection résultent de l'existence de divergences dans la transposition et l'application de la directive 95/46/CE.

(8) Afin d'assurer la cohérence et un degré élevé de protection des personnes, et de lever les obstacles à la circulation des données à caractère personnel, le niveau de protection des droits et des libertés des personnes à l'égard du traitement de ces données devrait être équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union.

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

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

(11) Afin d'obtenir un niveau uniforme de protection des personnes physiques dans toute l'Union, et d'éviter que des divergences n'entravent la libre circulation des données au sein du marché intérieur, un règlement est nécessaire pour garantir la sécurité juridique et la transparence aux opérateurs économiques, notamment les micro, petites et moyennes entreprises, pour assurer aux personnes de tous les États membres un même niveau de droits opposables, et des obligations et responsabilités égales pour les responsables du traitement des données et les sous-traitants, de même que pour assurer une surveillance cohérente du traitement des données à caractère personnel, des sanctions équivalentes dans tous les États membres et une coopération efficace entre les autorités de contrôle des différents États membres. Pour tenir compte de la situation particulière des micro, petites et moyennes entreprises, le présent règlement comporte un certain nombre de dérogations. Les institutions et organes de l'Union, les États membres et leurs autorités de contrôle sont, en outre, encouragés à prendre en considération les besoins spécifiques des micro, petites et moyennes entreprises dans le cadre l'application du présent règlement. Pour définir la notion de micro, petites et moyennes entreprises, il convient de s'inspirer de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises.

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

pouvoir être invoquée. Cela devrait être également le cas lorsque le nom de la personne morale contient le nom d'une ou plusieurs personnes physiques.

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

(14) Le présent règlement ne traite pas des questions de protection des libertés et droits fondamentaux ou de libre circulation des données relatives à des activités n'entrant pas dans le champ d'application du droit de l'Union; il ne couvre pas non plus le traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, qui relève du règlement (CE) n° 45/2001[44], ni celui qui est fait par les États membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union.

(15) Le présent règlement ne devrait pas s'appliquer aux traitements de données à caractère personnel effectués par une personne physique, par exemple un échange de correspondance ou la tenue d'un carnet d'adresses, qui sont exclusivement personnels ou domestiques et sans but lucratif, donc sans lien aucun avec une activité professionnelle ou commerciale. Elle ne devrait pas valoir non plus pour les responsables du traitement de données ou leurs sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.

(16) La protection des personnes physiques à l'égard du traitement des données à caractère personnel 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 la libre circulation de ces données font l'objet d'un instrument juridique spécifique au niveau de l'Union. Le présent règlement ne devrait donc pas s'appliquer aux activités de traitement effectuées à ces fins. Toutefois, le traitement de données à ces fins par des autorités publiques devrait être régi par cet instrument juridique plus spécifique au niveau de l'Union (à savoir la directive XX/YYY).

(17) Le présent règlement devrait s'appliquer sans préjudice de la directive 2000/31/CE, et notamment de ses articles 12 et 15 relatifs à la responsabilité des prestataires intermédiaires.

(18) Le présent règlement permet de prendre en compte, dans la mise en œuvre de ses dispositions, le principe du droit d'accès du public aux documents administratifs.

(19) Tout traitement de données à caractère personnel intervenant dans le cadre des activités d'un établissement d'un responsable du traitement ou sous-traitant situé sur le territoire de l'Union devrait être effectué conformément au présent règlement, que le traitement lui-même se déroule à l'intérieur de l'Union ou non. L'établissement

---

[44] JO L 8 du 12.01.2001, p. 1.

suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

(20) Afin d'éviter qu'une personne soit exclue de la protection qui lui est garantie en vertu du présent règlement, le traitement de données à caractère personnel concernant des personnes résidant dans l'Union, par un responsable du traitement qui n'est pas établi dans l'Union, devrait être soumis au présent règlement lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées, ou à l'observation de leur comportement.

(21) Afin de déterminer si une activité de traitement peut être considérée comme «observant le comportement» des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur l'internet au moyen de techniques de traitement de données consistant à appliquer un «profil» à un individu, afin notamment de prendre des décisions le concernant ou d'analyser ou de prévoir ses préférences, son comportement et sa disposition d'esprit.

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

(23) Il y a lieu d'appliquer les principes de protection à toute information concernant une personne identifiée ou identifiable. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne. Il n'y a pas lieu d'appliquer les principes de protection aux données qui ont été rendues suffisamment anonymes pour que la personne concernée ne soit plus identifiable.

(24) Lorsqu'elles utilisent des services en ligne, les personnes physiques se voient associer des identifiants en ligne tels que des adresses IP ou des témoins de connexion («cookies») par les appareils, applications, outils et protocoles utilisés. Ces identifiants peuvent laisser des traces qui, combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils et à identifier les personnes. Il en découle que des numéros d'identification, des données de localisation, des identifiants en ligne ou d'autres éléments spécifiques ne doivent pas nécessairement être considérés, en soi, comme des données à caractère personnel dans tous les cas de figure.

(25) Le consentement devrait être donné de manière explicite, selon toute modalité appropriée permettant une manifestation de volonté libre, spécifique et informée, consistant soit en une déclaration soit en un acte non équivoque de la personne concernée, garantissant qu'elle consent bien en toute connaissance de cause au traitement des données à caractère personnel, par exemple en cochant une case lorsqu'elle consulte un site internet ou par le biais de toute déclaration ou tout comportement indiquant clairement dans ce contexte qu'elle accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement tacite ou passif. Le consentement donné devrait valoir pour toutes les activités de traitement effectuées ayant la même finalité. Si le consentement de la

personne concernée est donné à la suite d'une demande par voie électronique, cette demande doit être claire, concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé.

(26) Les données à caractère personnel concernant la santé devraient comprendre, en particulier, l'ensemble des données se rapportant à l'état de santé d'une personne concernée; les informations relatives à l'enregistrement du patient pour la prestation de services de santé; les informations relatives aux paiements ou à l'éligibilité du patient à des soins de santé; un numéro ou un symbole attribué à un patient, ou des informations détaillées le concernant, destinés à l'identifier de manière univoque à des fins médicales; toute information relative au patient recueillie dans le cadre de la prestation de services de santé audit patient; des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des échantillons biologiques; l'identification d'une personne en tant que prestataire de soins de santé au patient; ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostique in vitro.

(27) Le principal établissement d'un responsable du traitement ou d'un sous-traitant 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, aux conditions et aux modalités du traitement dans le cadre d'une installation stable. Ce critère ne devrait pas dépendre du fait que le traitement ait effectivement lieu à cet endroit; la présence et l'utilisation de moyens techniques et de technologies permettant le traitement de données à caractère personnel ou la réalisation d'activités de ce type ne constituent pas en soi l'établissement principal ni, dès lors, un critère déterminant à cet égard. On entend par «établissement principal du sous-traitant» le lieu de son administration centrale dans l'Union.

(28) Un groupe d’entreprises devrait consister en une entreprise qui exerce le contrôle et des entreprises contrôlées, la première devant être celle qui peut exercer une influence dominante sur les autres du fait, par exemple, de la détention du capital, d'une participation financière ou des règles qui la régissent, ou du pouvoir de faire appliquer les règles relatives à la protection des données à caractère personnel.

(29) Les données à caractère personnel relatives aux enfants nécessitent une protection spécifique parce que ceux-ci peuvent être moins conscients des risques, des conséquences, des garanties et de leurs droits en matière de traitement des données. Afin de déterminer jusqu'à quel âge une personne est un enfant, le règlement devrait reprendre la définition retenue par la convention des Nations unies relative aux droits de l'enfant.

(30) Tout traitement de données à caractère personnel devrait être licite, loyal et transparent à l'égard des personnes concernées. En particulier, les finalités précises du traitement devraient être explicites et légitimes, et déterminées lors de la collecte des données. Les données devraient être adéquates, pertinentes et limitées au minimum nécessaire aux finalités pour lesquelles elles sont traitées, ce qui exige notamment de veiller à ce que les données collectées ne soient pas excessives et à ce que leur durée de conservation soit limitée au strict minimum. Les données à caractère personnel ne

devraient être traitées que si la finalité du traitement ne peut être atteinte par d'autres moyens. Il y a lieu de prendre toutes les mesures raisonnables afin que les données à caractère personnel qui sont inexactes soient rectifiées ou effacées. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement en vue de leur effacement ou d'une révision périodique.

(31) Pour être licite, le traitement devrait être fondé sur le consentement de la personne concernée ou sur tout autre fondement légitime prévu par la législation, soit dans le présent règlement soit dans un autre acte législatif de l'Union ou d'un État membre, ainsi que le prévoit le présent règlement.

(32) Lorsque le traitement est fondé sur le consentement de la personne concernée, c'est au responsable du traitement que devrait incomber la charge de prouver que ladite personne a bien consenti au traitement. En particulier, dans le contexte d'une déclaration écrite relative à une autre question, des garanties devraient faire en sorte que la personne concernée donne son consentement en toute connaissance de cause.

(33) Pour garantir que le consentement soit libre, il y aurait lieu de préciser qu'il ne constitue pas un fondement juridique valable si la personne ne dispose pas d'une véritable liberté de choix et n'est, dès lors, pas en mesure de refuser ou de se rétracter sans subir de préjudice.

(34) Le consentement ne devrait pas constituer un fondement juridique valable pour le traitement de données à caractère personnel lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, surtout lorsque la première se trouve dans une situation de dépendance par rapport au second, notamment lorsque les données à caractère personnel concernent le salarié et sont traitées par son employeur dans le cadre de leur relation de travail. Lorsque le responsable du traitement est une autorité publique, il n'y a déséquilibre que dans le cas d'opérations de traitement spécifiques dans le cadre desquelles l'autorité publique peut, en vertu de ses prérogatives de puissance publique, imposer une obligation. Dans ce cas, le consentement ne saurait être réputé librement consenti, compte tenu de l'intérêt de la personne concernée.

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

(36) Lorsque le traitement est réalisé conformément à une obligation légale à laquelle est soumis le responsable du traitement, ou lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt général ou relevant de l'exercice de l'autorité publique, le traitement devrait avoir son fondement juridique dans le droit de l'Union ou dans une loi nationale respectant les conditions imposées par la charte des droits fondamentaux de l'Union européenne pour toute limitation des droits et des libertés. Il appartient également au droit de l'Union ou à la loi nationale de déterminer si le responsable du traitement investi d'une mission d'intérêt général ou relevant de l'exercice de l'autorité publique doit être une administration publique ou une autre personne physique ou morale de droit public, ou de droit privé telle qu'une association professionnelle.

(37) Le traitement de données à caractère personnel devrait être également considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée.

(38) Les intérêts légitimes du responsable du traitement peuvent constituer un fondement juridique au traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée. Ce point mérite un examen attentif, surtout lorsque la personne concernée est un enfant, cette catégorie de personnes nécessitant en effet une protection spécifique. La personne concernée devrait pouvoir s'opposer au traitement des données la concernant, pour des raisons tenant à sa situation personnelle, et gratuitement. Afin d'assurer la transparence, le responsable du traitement devrait être tenu d'informer expressément la personne concernée des intérêts légitimes poursuivis, et de justifier ces derniers, ainsi que du droit de la personne de s'opposer au traitement. Étant donné qu'il appartient au législateur de fournir la base juridique autorisant les autorités publiques à traiter des données, ce motif ne devrait pas valoir pour les traitements effectués par ces autorités dans l'accomplissement de leur mission.

(39) Le traitement des données relatives au trafic, dans la mesure strictement nécessaire à la finalité de garantir la sécurité du réseau et des informations, c'est-à-dire la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées ou transmises, ainsi que la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par les pouvoirs publics, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes de réaction aux incidents touchant la sécurité informatique (CSIRT), des fournisseurs de réseaux ou de services de communications électroniques, par des fournisseurs de technologies et services de sécurité, constitue un intérêt légitime du responsable des données. 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.

(40) Le traitement des données à caractère personnel à d'autres fins ne devrait être autorisé que s'il est compatible avec les finalités de la collecte initiale des données, notamment lorsque le traitement est nécessaire à des fins statistiques ou de recherche historique ou scientifique. Lorsque cette autre finalité n'est pas compatible avec la finalité initiale de la collecte des données, il convient que le responsable du traitement obtienne le consentement de la personne concernée à cette autre finalité ou qu'il fonde le traitement sur un autre motif légitime, en particulier lorsque le droit de l'Union ou la législation de l'État membre dont relève le responsable des données le prévoit. En tout état de cause, l'application des principes énoncés par le présent règlement et, en particulier, de respecter l'obligation d'informer la personne concernée au sujet de ces autres finalités devrait être assurée.

(41) Les données à caractère personnel qui sont, par nature, particulièrement sensibles et vulnérables du point de vue des droits fondamentaux et de la vie privée méritent une protection spécifique. Ces données ne devraient pas faire l'objet d'un traitement, à moins que la personne concernée n'y consente expressément. Toutefois, des dérogations à cette interdiction devraient être expressément prévues pour tenir compte

de besoins spécifiques, en particulier lorsque le traitement a lieu dans le cadre d'activités légitimes de certaines associations ou fondations ayant pour finalité de permettre l'exercice des libertés fondamentales.

(42) Les exceptions à l'interdiction du traitement des catégories de données sensibles devraient également être autorisées si elles résultent d'une loi et, sous réserve de garanties appropriées, afin de protéger les données à caractère personnel et d'autres droits fondamentaux, dans le cas où des raisons d'intérêt général le justifient et, en particulier, à des fins de santé publique, en ce compris la protection de la santé, la protection sociale et la gestion des services de santé, notamment pour assurer la qualité et l'efficience des procédures de règlement des demandes de remboursement et de services dans le régime d'assurance-maladie, ou à des fins statistiques ou de recherche historique ou scientifique.

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

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

(45) Si les données qu'il traite ne lui permettent pas d'identifier une personne physique, le responsable du traitement ne devrait pas être tenu d'obtenir des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter une disposition du présent règlement. Dans le cas d'une demande d'accès, il devrait être autorisé à demander d'autres informations à la personne concernée, afin d'être en mesure de localiser les données personnelles que cette personne recherche.

(46) Le principe de transparence veut que toute information adressée au public ou à la personne concernée soit aisément accessible et facile à comprendre, et formulée en termes simples et clairs. Ceci vaut tout particulièrement lorsque, dans des domaines tels que la publicité en ligne, la multiplication des acteurs et la complexité des technologies utilisées empêchent la personne concernée de savoir exactement si des données à caractère personnel la concernant sont collectées, par qui et dans quel but. Les enfants nécessitant une protection spécifique, toute information et communication, lorsque le traitement des données les vise spécifiquement, devrait être rédigée en des termes simples et clairs que l'enfant peut aisément comprendre.

(47) Des modalités devraient être prévues pour faciliter l'exercice, par la personne concernée, des droits qui lui sont conférés par le présent règlement, notamment les moyens de demander sans frais l'accès aux données, leur rectification ou leur effacement, et d'exercer son droit d'opposition. Le responsable du traitement devrait être tenu de répondre à la personne concernée dans un délai donné et de motiver tout refus.

(48) Le principe de traitement loyal et transparent exige que la personne concernée soit informée, en particulier, de l'existence du traitement et de ses finalités, de la durée

pendant laquelle les données seront conservées, de l’existence d’un droit d’accès, de rectification ou d’effacement, ainsi que de son droit d'introduire une réclamation. Lorsque les données sont collectées auprès de la personne concernée, il importe que celle-ci sache également si elle est obligée de fournir ces informations et à quelles conséquences elle s'expose si elle ne les fournit pas.

(49) L'information sur le traitement des données à caractère personnel devrait être donnée à la personne concernée au moment où ces données sont recueillies ou, si la collecte des données n'a pas lieu auprès de la personne concernée, dans un délai raisonnable en fonction des circonstances propres à chaque cas. Lorsque des données peuvent être légitimement divulguées à un autre destinataire, il convient que la personne concernée soit informée lorsque ces données sont divulguées pour la première fois audit destinataire.

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

(51) Toute personne devrait avoir le droit d'accéder aux données qui ont été collectées à son sujet et d'exercer ce droit facilement, afin de s'informer du traitement qui en est fait et d'en vérifier la licéité. En conséquence, chaque personne concernée devrait avoir le droit de connaître et de se faire communiquer, en particulier, la finalité du traitement des données, la durée de leur conservation, l'identité des destinataires, la logique qui sous-tend le traitement des données et les conséquences qu'il pourrait avoir, au moins en cas de profilage. Ce droit ne devrait pas porter atteinte aux droits et libertés d’autrui, notamment au secret des affaires, ni à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Toutefois, ces considérations ne sauraient aboutir au refus de toute information de la personne concernée.

(52) Le responsable du traitement devrait prendre toutes les mesures raisonnables afin de s’assurer de l’identité d’une personne concernée demandant l'accès aux données, en particulier dans le contexte des services et identifiants en ligne. Un responsable des données ne devrait pas conserver des données à caractère personnel à la seule fin d'être en mesure de réagir à d'éventuelles demandes.

(53) Toute personne devrait avoir le droit de faire rectifier des données à caractère personnel la concernant, et disposer d'un «droit à l’oubli numérique» lorsque la conservation de ces données n'est pas conforme au présent règlement. En particulier, les personnes concernées devraient avoir le droit d'obtenir que leurs données soient effacées et ne soient plus traitées, lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été recueillies ou traitées, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de données à caractère personnel les concernant ou encore, lorsque le traitement de leurs données à caractère personnel n'est pas conforme au présent règlement. Ce droit est particulièrement important lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et donc mal

informée des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'internet. Toutefois, la conservation des données devrait être autorisée lorsqu'elle est nécessaire à des fins statistiques ou de recherche historique ou scientifique, pour des motifs d'intérêt général dans le domaine de la santé publique, ou à l'exercice du droit à la liberté d'expression, si elle est requise par la loi ou s'il existe une raison de limiter le traitement des données au lieu de les effacer.

(54) Afin de renforcer le «droit à l'oubli numérique» dans l'environnement en ligne, le droit à l'effacement des données devrait en outre être étendu de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques soit tenu d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données, ou toute copie ou reproduction de celles-ci. Afin d'assurer cette information, le responsable des données devrait prendre toutes les mesures raisonnables, y compris les mesures techniques, à l'égard des données dont la publication lui est imputable. En ce qui concerne la responsabilité de la publication de données à caractère personnel par un tiers, elle devrait être imputée au responsable du traitement lorsqu'il a lui-même autorisé le tiers à l'effectuer.

(55) Pour leur permettre de mieux maîtriser encore l'utilisation qui est faite des données les concernant et renforcer leur droit d'accès, les personnes devraient avoir le droit, lorsque des données à caractère personnel font l'objet d'un traitement automatisé dans un format structuré et couramment utilisé, d'obtenir une copie des données les concernant, également dans un format électronique structuré et couramment utilisé. La personne concernée devrait en outre être autorisée à transférer ces données, qu'elle a fournies, d'une application automatisée, telle qu'un réseau social, à une autre. Ce droit devrait s'appliquer lorsque la personne concernée a fourni les données au système de traitement automatisé, en donnant son consentement ou dans le cadre de l'exécution d'un contrat.

(56) Dans les cas où des données à caractère personnel pourraient faire l'objet d'un traitement licite afin de protéger les intérêts vitaux de la personne concernée, ou pour un motif d'intérêt général, à l'exercice de l'autorité publique ou à la poursuite des intérêts légitimes du responsable du traitement, toute personne concernée devrait néanmoins avoir le droit de s'opposer au traitement de toute donnée la concernant. Il devrait incomber au responsable du traitement de prouver que ses intérêts légitimes prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée.

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

(58) Toute personne physique devrait avoir le droit de ne pas être soumise à une mesure fondée sur le profilage par traitement automatisé. Toutefois, de telles mesures devraient être permises lorsqu'elles sont expressément autorisées par la loi, appliquées dans le cadre de la conclusion ou de l'exécution d'un contrat, ou si la personne concernée y a donné son consentement. En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, y compris une information spécifique de la personne concernée et le droit d'obtenir une intervention humaine, et cette mesure ne devrait pas concerner les enfants.

(59) Des limitations des principes spécifiques et du droit à l'information, du droit d'accès, de rectification et d'effacement, ou du droit à la portabilité des données, du droit d'opposition, des mesures fondées sur le profilage, ainsi que de la communication d'une violation des données à caractère personnel à une personne concernée, et des limitations de certaines obligations connexes des responsables du traitement des données peuvent être imposées par le droit de l'Union ou d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique, pour garantir la sécurité publique, notamment aux fins de la protection de la vie humaine en cas, plus particulièrement, de catastrophe d'origine naturelle ou humaine, aux fins de la prévention, de l'investigation et de la poursuite d'infractions pénales ou de manquements à la déontologie des professions réglementées, aux fins d'autres intérêts publics, y compris d'un intérêt économique ou financier important de l'Union ou d'un État membre, ou aux fins de la protection de la personne concernée ou des droits ou libertés de tiers. Ces limitations doivent être conformes aux exigences énoncées par la charte des droits fondamentaux de l'Union européenne et par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

(60) Il y a lieu d'instaurer une responsabilité globale 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 veille à la conformité de chaque traitement au présent règlement et soit tenu d'en apporter la preuve.

(61) La protection des droits et libertés des personnes concernées à l'égard du traitement des données à caractère personnel nécessite de prendre les mesures techniques et organisationnelles appropriées, tant au moment de la conception que de l'exécution du traitement, de sorte que les exigences du présent règlement soient respectées. Afin d'assurer et de démontrer la conformité de ses activités au présent règlement, le responsable du traitement devrait adopter des règles internes et appliquer des mesures adaptées, qui répondent en particulier aux principes de la protection des données dès la conception et de la protection des données par défaut.

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

(63) Lorsqu'un responsable du traitement qui n'est pas établi dans l'Union traite des données à caractère personnel concernant des personnes résidant dans l'Union, et que les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, ou à l'observation de leur comportement, il conviendrait que le responsable du traitement désigne un représentant, à moins que ledit responsable ne soit établi dans un pays tiers qui assure un niveau de protection adéquat, ou que le responsable ne soit une petite ou moyenne entreprise ou une autorité ou un organisme public, ou qu'il ne propose qu'occasionnellement des biens ou des services à ces personnes concernées. Le représentant devrait agir pour le compte du responsable du traitement et devrait pouvoir être contacté par toute autorité de contrôle.

(64) Afin de déterminer si un responsable des données n'offre qu'occasionnellement des biens et des services à des personnes concernées résidant dans l'Union, il y aurait lieu de vérifier s'il ressort de l'ensemble de ses activités que l'offre de biens et de services à ces personnes concernées est accessoire à ses activités principales.

(65) Afin d'apporter la preuve qu'il se conforme au présent règlement, le responsable du traitement ou le sous-traitant devrait consigner chaque opération de traitement. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces informations à sa disposition sur demande pour qu'elles servent au contrôle des opérations en question.

(66) Afin de préserver la sécurité et de prévenir tout traitement contraire au présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et prenne des mesures pour les atténuer. Ces mesures devraient assurer un niveau de sécurité approprié compte tenu, d'une part, de l'état de la technique et de leur coût de mise en œuvre, et, d'autre part, des risques présentés par les traitements et de la nature des données à protéger. Lors de l'adoption de normes techniques et de mesures organisationnelles destinées à garantir la sécurité du traitement, la Commission devrait promouvoir la neutralité technologique, l'interopérabilité et l'innovation, et au besoin, coopérer avec les pays tiers.

(67) Une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer une grave perte économique et des dommages sociaux importants, y compris une usurpation d'identité, à la personne physique concernée. En conséquence, dès que le responsable du traitement apprend qu'une telle violation s'est produite, il conviendrait qu'il en informe l'autorité de contrôle sans retard injustifié et, lorsque c'est possible, dans les 24 heures. Si ce délai ne peut être respecté, la notification devrait être assortie d'une explication concernant ce retard. Les personnes physiques dont les données à caractère personnel pourraient être affectées par la violation devraient en être averties sans retard injustifié afin de pouvoir prendre les précautions qui s'imposent. Il y a lieu de considérer qu'une violation affecte les données à caractère personnel ou la vie privée d'une personne concernée lorsqu'il peut en résulter, par exemple, un vol ou une usurpation d'identité, un dommage physique, une humiliation grave ou une atteinte à la réputation. La notification devra décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne concernée afin d'atténuer les éventuels effets négatifs. Il convient que les notifications aux personnes concernées soient effectuées aussi rapidement que possible, en coopération étroite avec l'autorité de contrôle, et dans le respect des directives fournies par celle-ci ou par d'autres autorités compétentes (telles que les autorités répressives). Par exemple, pour que les personnes concernées puissent atténuer un risque immédiat de préjudice, il faudrait leur adresser une notification le plus rapidement possible, mais la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données ou la survenance de violations similaires pourrait justifier un délai plus long.

(68) Afin de déterminer si une violation des données à caractère personnel est notifiée sans retard injustifié à l'autorité de contrôle et à la personne concernée, il y a lieu de vérifier si le responsable du traitement a mis en place et appliqué une protection technologique et des mesures d'organisation appropriées pour établir immédiatement si une violation des données est intervenue et pour informer dans les meilleurs délais l'autorité de contrôle et la personne concernée, avant qu'une atteinte ne soit portée aux intérêts

personnels ou économiques de la personne, compte tenu notamment de la nature et de la gravité de la violation des données et de ses conséquences et effets néfastes pour la personne concernée.

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

(70) La directive 95/46/CE prévoyait une obligation générale de notifier les traitements de données à caractère personnel aux autorités de contrôle. Or cette obligation génère une charge administrative et financière, sans pour autant avoir véritablement amélioré la protection des données. En conséquence, l'obligation générale de notification devrait être supprimée et remplacée par des procédures et des mécanismes efficaces ciblant plutôt les traitements susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées, du fait de leur nature, de leur portée ou de leur finalité. Dans de tels cas, une analyse d'impact relative à la protection des données devrait être réalisée par le responsable du traitement ou le sous-traitant, préalablement au traitement, et devrait examiner notamment les dispositions, garanties et mécanismes envisagés pour assurer la protection des données à caractère personnel et pour démontrer que le présent règlement est respecté.

(71) Ceci devrait s'appliquer en particulier aux systèmes d'archivage à grande échelle récemment créés, qui servent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational et pourraient affecter un nombre important de personnes concernées.

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

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

(74) Lorsqu'une analyse d'impact relative à la protection des données indique que des opérations de traitement exposent les droits et libertés des personnes concernées à un degré élevé de risques particuliers, comme priver ces personnes d'un droit, ou de par l'utilisation de certaines technologies nouvelles, l'autorité de contrôle devrait pouvoir être consultée, avant le début de l'opération, sur un traitement risqué susceptible de ne

pas être conforme au présent règlement, et formuler des propositions visant à y remédier. Cette consultation devrait également avoir lieu pendant l'élaboration d'une mesure législative du parlement national, ou d'une mesure fondée sur cette dernière définissant la nature du traitement et instaurant les garanties appropriées.

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

(76) Il y a lieu d'encourager les associations et autres instances représentatives des responsables de traitement de données à élaborer des codes de conduite, dans le respect du présent règlement, de manière à faciliter sa bonne application, en tenant compte des spécificités des traitements effectués dans certains secteurs.

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

(78) La circulation transfrontière des données à caractère personnel est nécessaire au développement de la coopération internationale et du commerce mondial. L'augmentation de ces flux a cependant créé de nouveaux enjeux et de nouvelles préoccupations en ce qui concerne la protection des données à caractère personnel. Or il importe que, lorsque ces données sont transférées de l'Union vers des pays tiers ou à des organisations internationales, le niveau de protection des personnes physiques garanti dans l'Union par le présent règlement ne soit pas amoindri. En tout état de cause, les transferts vers des pays tiers ne peuvent avoir lieu que dans le plein respect du présent règlement.

(79) Le présent règlement ne remet pas en cause les accords internationaux conclus entre l'Union et les pays tiers en vue de réglementer le transfert des données à caractère personnel, y compris les garanties appropriées au bénéfice des personnes concernées.

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

(81) Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait, dans son évaluation du pays tiers, prendre en considération la manière dont ce pays respecte l'État de droit, garantit

l’accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme.

(82) La Commission peut également constater qu’un pays tiers, un territoire ou un secteur de traitement de données dans un pays tiers, ou une organisation internationale n'offre pas un niveau adéquat de protection des données. Si tel est le cas, le transfert de données à caractère personnel vers ce pays tiers devrait être interdit. Il y aurait alors lieu de prendre des dispositions en vue d'une consultation entre la Commission et le pays tiers ou l'organisation internationale.

(83) En l’absence de décision constatant le caractère adéquat du niveau de protection, 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 celle-ci, ou d'autres mesures adaptées et proportionnées qui se justifient au regard des circonstances qui entourent une opération ou une série d'opérations de transfert de données, et dans les cas autorisés par une autorité de contrôle.

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

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

(86) Le présent règlement devrait autoriser les transferts dans certains cas où la personne concernée a donné son consentement, lorsque le transfert est nécessaire dans le cadre d'un contrat ou d'une action en justice, lorsque des motifs importants d'intérêt général établis par le droit de l'Union ou d'un État membre l'exigent, ou lorsque le transfert est effectué à partir d'un registre établi par la loi et destiné à être consulté par le public ou par des personnes y ayant un intérêt légitime. Dans ce dernier cas de figure, le transfert ne devrait toutefois pas porter sur la totalité des données ni sur des catégories entières de données contenues dans le registre et, lorsque ce dernier est destiné à être consulté par des personnes qui y ont un intérêt légitime, le transfert ne devrait avoir lieu que si ces personnes le demandent ou si elles en sont les destinataires.

(87) Ces dérogations devraient s'appliquer en particulier aux transferts de données qui sont nécessaires à la protection pour des motifs importants d'intérêt général, par exemple en cas de transfert international de données entre autorités de la concurrence, administrations fiscales ou douanières, entre autorités de surveillance financière, entre services chargés des questions de sécurité sociale, ou en cas de transfert aux autorités

compétentes chargées de la prévention et de la détection des infractions pénales, des enquêtes et des poursuites en la matière.

(88) Les transferts qui ne peuvent être qualifiés de fréquents ou massifs pourraient également être autorisés aux fins de la poursuite des intérêts légitimes du responsable du traitement ou du sous-traitant, après que ces derniers ont évalué toutes les circonstances entourant le transfert. Pour les traitements à des fins historiques, statistiques et de recherche scientifique, il y aurait lieu de prendre en considération les attentes légitimes de la société en matière de progrès des connaissances.

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

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

(91) Lorsque des données à caractère personnel franchissent les frontières, elles accroissent le risque que les personnes physiques ne puissent exercer leur droit à la protection des données, notamment pour se protéger de l'utilisation ou la divulgation illicite de ces informations. De même, les autorités de contrôle peuvent être confrontées à l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités exercées en dehors de leurs frontières. Leurs efforts pour collaborer dans le contexte transfrontière peuvent également être freinés par les pouvoirs insuffisants dont elles disposent, par l'hétérogénéité des régimes juridiques et par des obstacles pratiques tels que le manque de ressources. En conséquence, il est nécessaire de favoriser une coopération plus étroite entre les autorités de contrôle de la protection des données, afin qu'elles puissent échanger des informations et mener des enquêtes avec leurs homologues internationaux.

(92) L'institution d'autorités de contrôle dans les États membres, exerçant leurs fonctions en toute indépendance, est un élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Les États membres ont la possibilité d'instituer plusieurs autorités de contrôle, pour s'aligner sur leur structure constitutionnelle, organisationnelle et administrative.

(93) Lorsqu'un État membre crée plusieurs autorités de contrôle, il devrait prévoir, dans sa législation, des dispositifs garantissant la participation effective de ces autorités au

mécanisme de contrôle de la cohérence. Il devrait en particulier désigner l'autorité de contrôle qui servira de point de contact unique, permettant une participation efficace de ces autorités au mécanisme, afin d'assurer une coopération rapide et facile avec les autres autorités de contrôle, le comité européen de la protection des données et la Commission.

(94) Il conviendrait que chaque autorité de contrôle soit dotée de tous les moyens financiers et humains, les locaux et les infrastructures nécessaires à la bonne exécution de ses tâches, 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.

(95) Les conditions générales applicables aux membres de l'autorité de contrôle devraient être fixées par la loi dans chaque État membre, prévoir notamment que ces membres sont nommés par le parlement ou par le gouvernement national, et comprendre des dispositions régissant la qualification et la fonction de ces membres.

(96) Il appartiendrait aux autorités de contrôle de surveiller l'application des dispositions du présent règlement et de contribuer à ce que cette application soit uniforme dans l'ensemble de l'Union, pour protéger les personnes physiques à l'égard du traitement de leurs données à caractère personnel et faciliter la libre circulation de ces données au sein du marché intérieur. À cet effet, il conviendrait que les autorités de contrôle coopèrent entre elles et avec la Commission.

(97) Lorsque, dans l'Union, le traitement de données à caractère personnel intervenant dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant a lieu dans plusieurs États membres, il conviendrait qu'une seule autorité de contrôle soit compétente pour surveiller les activités du responsable du traitement ou du sous-traitant dans toute l'Union et pour prendre les décisions y afférentes, afin de favoriser une application cohérente, de garantir la sécurité juridique et de réduire les charges administratives pour le responsable du traitement et ses sous-traitants.

(98) L'autorité compétente faisant ainsi office de guichet unique devrait être l'autorité de contrôle de l'État membre dans lequel le responsable du traitement ou le sous-traitant a son principal établissement.

(99) Bien que le présent règlement s'applique également aux activités des juridictions nationales, la compétence des autorités de contrôle ne devrait pas s'étendre aux traitements de données à caractère personnel effectués par les juridictions lorsqu'elles agissent dans le cadre de leur fonction juridictionnelle, afin de préserver l'indépendance des juges dans le cadre de leur fonction juridictionnelle. Il conviendrait toutefois que cette exception soit strictement limitée aux activités purement judiciaires intervenant dans le cadre d'affaires portées devant les tribunaux et qu'elle ne s'applique pas aux autres activités auxquelles les juges pourraient être associés en vertu du droit national.

(100) Afin d'assurer la cohérence du contrôle et de l'application du présent règlement dans l'ensemble de l'Union, les autorités de contrôle devraient avoir, dans chaque État membre, les mêmes missions et pouvoirs effectifs, dont des pouvoirs d'enquête, d'intervention juridiquement contraignante, de décision et de sanction, en particulier en cas de réclamation introduite par des personnes physiques, ainsi que le pouvoir d'ester en justice. Les pouvoirs d'investigation des autorités de contrôle en matière d'accès aux

locaux devraient être exercés conformément au droit de l'Union et au droit national applicable. Cela concerne en particulier de l'obligation d'obtenir préalablement une autorisation judiciaire.

(101) Chaque autorité devrait recevoir les réclamations des personnes concernées et examiner les affaires en question. L'enquête faisant suite à une réclamation devrait être menée, sous contrôle juridictionnel, dans la mesure appropriée requise par l'affaire. L'autorité de contrôle devrait informer la personne concernée de l'état d'avancement et du résultat de la réclamation dans un délai raisonnable. Si l'affaire requiert un complément d'enquête ou une coordination avec une autre autorité de contrôle, des informations intermédiaires devraient être fournies à la personne concernée.

(102) Les activités de sensibilisation organisées par les autorités de contrôle à l'intention du public devraient comprendre des mesures spécifiques aux responsables du traitement et aux sous-traitants, y compris les micro, petites et moyennes entreprises, et aux personnes concernées.

(103) Les autorités de contrôle devraient se prêter mutuellement assistance dans l'exercice de leurs fonctions afin d'assurer une application cohérente du présent règlement dans le marché intérieur.

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

(105) Afin de garantir l'application cohérente du présent règlement dans toute l'Union, il y a lieu d'instaurer un mécanisme de contrôle de la cohérence encadrant la coopération entre les autorités de contrôle elles-mêmes et avec la Commission. Ce mécanisme devrait notamment s'appliquer lorsqu'une autorité de contrôle a l'intention de prendre une mesure à l'égard d'opérations de traitement qui sont liées à l'offre de biens ou de services à des personnes concernées se trouvant dans plusieurs États membres, ou à l'observation de ces personnes, ou qui pourraient affecter considérablement la libre circulation des données à caractère personnel. Il devrait également s'appliquer lorsqu'une autorité de contrôle ou la Commission demande qu'une question soit traitée dans ce cadre. Le mécanisme devrait s'appliquer sans préjudice des éventuelles mesures que la Commission pourrait prendre dans l'exercice des pouvoirs que lui confèrent les traités.

(106) En application du mécanisme de contrôle de la cohérence, le comité européen de la protection des données devrait émettre un avis, dans un délai déterminé, si une majorité simple de ses membres le décide ou s'il est saisi d'une demande en ce sens par une autorité de contrôle ou par la Commission.

(107) Afin de garantir le respect du présent règlement, la Commission peut adopter un avis sur cette question, ou une décision ordonnant à l'autorité de contrôle de suspendre son projet de mesure.

(108) Il peut être nécessaire d'agir de toute urgence pour protéger les intérêts des personnes concernées, en particulier lorsque l'exercice du droit d'une personne concernée risque d'être considérablement entravé. En conséquence, lorsqu'elle applique le mécanisme

de contrôle de la cohérence, l'autorité de contrôle devrait pouvoir adopter des mesures provisoires d'une durée déterminée.

(109) L'application de ce mécanisme devrait conditionner la validité juridique et l'exécution de la décision par une autorité de contrôle. Dans d'autres cas présentant une dimension transfrontière, les autorités de contrôle concernées pourraient se prêter mutuellement assistance et mener des enquêtes conjointes sur une base bilatérale ou multilatérale, sans actionner le mécanisme de contrôle de la cohérence.

(110) Un comité européen de la protection des données devrait être créé au niveau de l'Union. Il devrait remplacer le 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. Il devrait se composer d'un directeur d'une autorité de contrôle de chaque État membre et du contrôleur européen de la protection des données. La Commission devrait participer à ses activités. Le comité européen de la protection des données devrait contribuer à l'application cohérente du présent règlement dans toute l'Union, notamment en conseillant la Commission et en favorisant la coopération des autorités de contrôle dans l'ensemble de l'Union. Il devrait exercer ses fonctions en toute indépendance.

(111) Toute personne concernée devrait avoir le droit d'introduire une réclamation auprès d'une autorité de contrôle dans tout État membre et disposer d'un droit de recours si elle estime que les droits que lui confère le présent règlement ne sont pas respectés, si l'autorité de contrôle ne réagit pas à une réclamation ou si elle n'agit pas alors qu'une action est nécessaire pour protéger les droits de la personne concernée.

(112) Tout organisme, organisation ou association qui œuvre à la protection des droits et intérêts des personnes concernées dans le domaine de la protection des données et qui est constitué(e) conformément au droit d'un État membre devrait avoir le droit d'introduire une réclamation auprès d'une autorité de contrôle ou d'exercer le droit de recours au nom de personnes concernées, ou d'introduire une réclamation en son propre nom, indépendamment de celle d'une personne concernée, dans les cas où l'organisme, l'organisation ou l'association considère qu'une violation de données à caractère personnel a été commise.

(113) Toute personne physique ou morale devrait disposer d'un droit de recours contre les décisions d'une autorité de contrôle qui la concernent. Les actions contre une autorité de contrôle devraient être intentées devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie.

(114) Afin de renforcer la protection judiciaire de la personne concernée dans les cas où l'autorité de contrôle compétente est établie dans un autre État membre que celui dans lequel la personne concernée réside, cette dernière peut demander à tout organisme, organisation ou association œuvrant à la protection des droits et intérêts des personnes concernées en vue de protéger leurs données à caractère personnel, d'intenter, pour son compte, un recours contre l'autorité de contrôle en question devant la juridiction compétente de l'autre État membre.

(115) Dans le cas où l'autorité de contrôle compétente établie dans un autre État membre n'agit pas ou a pris des mesures insuffisantes au sujet d'une réclamation, la personne concernée peut demander à l'autorité de contrôle de l'État membre dans lequel elle

réside habituellement d'intenter une action contre l'autorité de contrôle défaillante, devant la juridiction compétente de l'autre État membre. L'autorité de contrôle requise peut décider, sous contrôle juridictionnel, s'il y a lieu ou non de faire droit à la demande.

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

(117) S'il existe des raisons de penser que des procédures parallèles sont pendantes devant les juridictions de différents États membres, ces juridictions devraient être tenues de prendre contact les unes avec les autres. Les juridictions devraient avoir la possibilité de surseoir à statuer lorsqu'une affaire parallèle est pendante dans un autre État membre. Les États membres devraient veiller à ce que les actions en justice, pour être efficaces, permettent l'adoption rapide de mesures visant à réparer ou à prévenir une violation du présent règlement.

(118) Tout dommage qu'une personne pourrait subir du fait d'un traitement illicite devrait être réparé par le responsable du traitement ou le sous-traitant, qui peut cependant s'exonérer de sa responsabilité s'il prouve que le dommage ne lui est pas imputable, notamment s'il établit l'existence d'une faute de la personne concernée, ou en cas de force majeure.

(119) Toute personne de droit privé ou de droit public qui ne respecte pas le présent règlement devrait faire l'objet de sanctions pénales. Les États membres devraient veiller à ce que les sanctions soient effectives, proportionnées et dissuasives, et prendre toutes mesures nécessaires à leur application.

(120) 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 de sanctionner les infractions administratives. Le présent règlement devrait définir ces infractions ainsi que le montant maximal des amendes administratives dont elles sont passibles. Le montant de l'amende devrait être fixé, dans chaque cas, en fonction de la situation spécifique, compte dûment tenu, notamment, de la nature, de la gravité et de la durée de l'infraction. Il pourrait en outre être recouru au mécanisme de contrôle de la cohérence pour résoudre les divergences d'application des sanctions administratives.

(121) Le traitement de données à caractère personnel à des fins uniquement journalistiques ou aux fins d'expression artistique ou littéraire devrait pouvoir bénéficier d'une dérogation à certaines dispositions du présent règlement, pour concilier le droit à la protection de ces données avec le droit à la liberté d'expression, et notamment le droit de recevoir et de communiquer des informations, garanti en particulier par l'article 11 de la charte des droits fondamentaux de l'Union européenne. Ceci devrait notamment s'appliquer aux traitements de données à caractère personnel dans le domaine de l'audiovisuel et dans les documents d'archives et bibliothèques de journaux. En conséquence, les États membres devraient adopter des mesures législatives qui prévoient les exemptions et dérogations nécessaires pour assurer l'équilibre avec ces droits fondamentaux. Les États membres devraient adopter de telles exemptions et

dérogations en ce qui concerne les principes généraux, les droits de la personne concernée, le responsable des données et le sous-traitant, le transfert des donnés vers des pays tiers ou à des organisations internationales, les autorités de contrôle indépendantes, et la coopération et la cohérence. Néanmoins, ceci ne devrait pas conduire les États membres à prévoir des dérogations aux autres dispositions du présent règlement. Pour tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique, il y a lieu de retenir une interprétation large des notions liées à cette liberté, comme le journalisme. Par conséquent, aux fins des exemptions et dérogations à établir en vertu du présent règlement, les États membres devraient qualifier de «journalistiques» les activités ayant pour objet de communiquer au public des informations, des opinions ou des idées, quel que soit le vecteur utilisé pour les transmettre. Il convient de ne pas limiter cette catégorie aux seules activités des entreprises de médias et d'y inclure tant celles qui poursuivent un but lucratif que celles qui n'en poursuivent pas.

(122) Le traitement des données à caractère personnel concernant la santé, qui constituent une catégorie spéciale de données exigeant une protection plus élevée, peut souvent être justifié par divers motifs légitimes, dans l'intérêt des personnes et de la société dans son ensemble, notamment lorsqu'il s'agit d'assurer la continuité des soins de santé d'un pays à un autre. Le présent règlement devrait donc prévoir des conditions harmonisées pour le traitement des données à caractère personnel dans le domaine de la santé, en les assortissant de garanties spécifiques et appropriées pour protéger les droits fondamentaux et les données à caractère personnel des personnes physiques. Ceci inclut leur droit d'accéder aux données ayant trait à leur santé, par exemple les données des dossiers médicaux faisant état de diagnostics, de résultats d'examens, d'avis de médecins traitants ou de tout traitement ou intervention effectués.

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

(124) Les principes généraux concernant la protection des personnes physiques à l’égard du traitement des données à caractère personnel devraient également être applicables dans le contexte de l'emploi. En conséquence, pour réglementer le traitement des données à caractère personnel des salariés dans ce contexte, les États membres devraient pouvoir, dans les limites du présent règlement, adopter par voie législative des règles spécifiques au traitement des données à caractère personnel dans le secteur de l’emploi.

(125) Le traitement de données à caractère personnel à des fins statistiques ou de recherche historique ou scientifique devrait, pour être licite, également respecter d'autres législations pertinentes, telles que celle relative aux essais cliniques.

(126) Aux fins du présent règlement, la notion de «recherche scientifique» devrait comprendre la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé, et devrait en outre tenir compte de l'objectif de l'Union mentionné à l'article 179, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, consistant à réaliser un espace européen de la recherche.

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

(128) Conformément à l'article 17 du traité sur le fonctionnement de l'Union européenne, le présent règlement respecte et ne préjuge pas du statut dont bénéficient, en vertu du droit national, les églises et les associations ou communautés religieuses dans les États membres. Il s'ensuit que si, dans un État membre, une église applique, à la date d'entrée en vigueur du présent règlement, un ensemble complet de règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, ces règles existantes devraient continuer de s'appliquer si elles sont mises en conformité avec les dispositions du présent règlement. Ces églises et les associations religieuses devraient être tenues d'instituer une autorité de contrôle totalement indépendante.

(129) Afin de remplir les objectifs du présent règlement, à savoir la protection des droits et libertés fondamentaux des personnes physiques, et en particulier de leur droit à la protection des données à caractère personnel, et pour garantir la libre circulation de ces dernières au sein de l'Union, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission. Concrètement, des actes délégués devraient être adoptés en ce qui concerne la licéité du traitement; la spécification des critères et conditions concernant le consentement des enfants; les traitements portant sur des catégories particulières de données; la spécification des critères et conditions applicables aux demandes manifestement excessives et des frais facturés à la personne concernée pour exercer ses droits; les critères et les exigences applicables à l'information de la personne concernée et au droit d'accès; le droit à l'oubli numérique et à l'effacement; les mesures fondées sur le profilage; les critères et exigences en rapport avec les obligations incombant au responsable du traitement et avec la protection des données dès la conception ou par défaut; les sous-traitants; les critères et exigences spécifiques pour la documentation et la sécurité du traitement; les critères et exigences en vue d'établir une violation des données à caractère personnel et de la notifier à l'autorité de contrôle, et les cas dans lesquels une violation des données à caractère personnel est susceptible de porter préjudice à la personne concernée; les critères et conditions déterminant la nécessité d'une analyse d'impact en ce qui concerne des opérations de traitement; les critères et exigences pour établir l'existence d'un degré élevé de risques spécifiques justifiant une consultation préalable; la désignation et les missions du délégué à la

protection des données; les codes de conduite; les critères et exigences applicables aux mécanismes de certification; les transferts encadrés par des règles d'entreprise contraignantes les dérogations relatives aux transferts; les sanctions administratives; les traitements à des fins médicales; les traitements dans le contexte professionnel et les traitements à des fins historiques, statistiques et de recherche scientifique. Il importe particulièrement que la Commission procède aux consultations appropriées tout au long de son travail préparatoire, y compris au niveau des experts. Durant la phase de préparation et de rédaction des actes délégués, la Commission devrait transmettre simultanément, en temps utile et en bonne et due forme, les documents pertinents au Parlement européen et au Conseil.

(130) Afin de garantir des conditions uniformes pour la mise en œuvre du présent règlement, il y aurait lieu de conférer des compétences d'exécution à la Commission pour qu'elle définisse les formulaires types relatifs au traitement des données à caractère personnel des enfants; des procédures et formulaires types pour l'exercice des droits de la personne concernée; des formulaires types pour l'information de la personne concernée; les formulaires types et les procédures pour le droit d'accès et le droit à la portabilité des données; des formulaires types concernant les obligations du responsable du traitement en matière de protection des données dès la conception, de protection des données par défaut, et de documentation; des exigences spécifiques relatives à la sécurité du traitement des données; de la forme normalisée et des procédures pour la notification des violations de données à caractère personnel à l'autorité de contrôle, et pour la communication d'une violation des données à caractère personnel à la personne concernée; des critères et procédures pour l'analyse d'impact relative à la protection de données; des formulaires et des procédures d'autorisation et de consultation préalables; des normes techniques et des mécanismes de certification; du niveau de protection adéquat offert par un pays tiers, par un territoire ou un secteur de traitement de données dans ce pays tiers, ou par une organisation internationale; des divulgations non autorisées par le droit de l'Union; de l'assistance mutuelle; des opérations conjointes; les décisions relevant du mécanisme de contrôle de la cohérence. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission[45]. Dans ce cadre, la Commission devrait envisager des mesures spécifiques pour les micro, petites et moyennes entreprises.

(131) La procédure d'examen devrait être appliquée pour l'établissement des formulaires types en vue de l'obtention du consentement d'un enfant; des procédures et formulaires types pour l'exercice des droits de la personne concernée; des formulaires types pour l'information de la personne concernée; des formulaires types et des procédures pour le droit d'accès et le droit à la portabilité des données; des formulaires types concernant les obligations du responsable du traitement en matière de protection des données dès la conception, de protection des données par défaut, et de documentation; des exigences spécifiques relatives à la sécurité du traitement des données; de la forme normalisée et des procédures pour la notification des violations de données à caractère

[45] Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

personnel à l'autorité de contrôle, et pour la communication d'une violation des données à caractère personnel à la personne concernée; des critères et procédures pour l'analyse d'impact relative à la protection de données; des formulaires et des procédures d'autorisation et de consultation préalables; des normes techniques et des mécanismes de certification; du niveau de protection adéquat offert par un pays tiers, par un territoire ou un secteur de traitement de données dans ce pays tiers, ou par une organisation internationale; des divulgations non autorisées par le droit de l'Union; de l'assistance mutuelle; des opérations conjointes; et pour l'adoption des décisions relevant du mécanisme de contrôle de la cohérence, puisque ces actes sont de portée générale.

(132) La Commission devrait adopter des actes d'exécution immédiatement applicables lorsque, dans des cas dûment justifiés concernant un pays tiers, ou un territoire ou secteur de traitement de données dans ce pays tiers, ou une organisation internationale, qui n'assure pas un niveau de protection adéquat, ou concernant des questions communiquées par les autorités de contrôle dans le cadre du mécanisme de contrôle de la cohérence, des raisons d'urgence impérieuses l'exigent.

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

(134) La directive 95/46/CE devrait être abrogée par le présent règlement. Néanmoins, les décisions de la Commission qui ont été adoptées, et les autorisations qui ont été accordées par les autorités de contrôle, sur le fondement de ladite directive devraient demeurer en vigueur.

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

(136) En ce qui concerne l'Islande et la Norvège, le présent règlement constitue un développement des dispositions de l'acquis de Schengen, dans la mesure où il s'applique au traitement des données à caractère personnel par les autorités participant à la mise en œuvre de cet acquis, au sens de l'accord conclu par le Conseil de l'Union européenne, et la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[46].

[46] JO L 176 du 10.7.1999, p. 36.

(137) En ce qui concerne la Suisse, le présent règlement constitue un développement des dispositions de l'acquis de Schengen, dans la mesure où il s'applique au traitement des données à caractère personnel par les autorités participant à la mise en œuvre de cet acquis, au sens de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[47].

(138) En ce qui concerne le Liechtenstein, le présent règlement constitue un développement des dispositions de l'acquis de Schengen dans la mesure où il s'applique au traitement des données à caractère personnel par les autorités participant à la mise en œuvre de cet acquis, au sens du protocole signé entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[48].

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

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.

---

47 JO L 53 du 27.2.2008, p. 52.
48 JO L 160 du 18.6.2011, p. 19.

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

Article 2
Champ d'application matériel

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

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

   a) dans le cadre d'une activité n'entrant pas dans le champ d'application du droit de l'Union, en ce qui concerne notamment la sécurité nationale;

   b) par les institutions, organes et organismes de l'Union;

   c) par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 2 du traité sur l'Union européenne;

   d) par une personne physique sans but lucratif dans le cadre de ses activités exclusivement personnelles ou domestiques;

   e) 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.

3. Le présent règlement s'applique sans préjudice de la directive 2000/31/CE, et en particulier des dispositions des articles 12 à 15 de ladite directive établissant les règles en matière de responsabilité des prestataires 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 de données ou d'un sous-traitant sur le territoire de l'Union.

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

   a) à l'offre de biens ou de services à ces personnes concernées dans l'Union; ou

   b) à l'observation de leur comportement.

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

Article 4
Définitions

Aux fins du présent règlement, on entend par:

(1) «personne concernée»: une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

(2) «données à caractère personnel»: toute information se rapportant à une personne concernée;

(3) «traitement de données à caractère personnel»: toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés, et appliquée(s) à des données à caractère personnel, telle(s) 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, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que l'effacement ou la destruction;

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

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

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

(7) «destinataire»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel;

(8) «consentement de la personne concernée»: toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne concernée accepte, par une

déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

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

(10) «données génétiques»: toutes les données, de quelque nature que ce soit, concernant les caractéristiques d'une personne physique qui sont héréditaires ou acquises à un stade précoce de son développement prénatal;

(11) «données biométriques»: toutes les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques;

(12) «données concernant la santé»: toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne;

(13) «établissement principal»: en ce qui concerne le responsable du traitement, le lieu de son établissement dans l'Union où sont prises les principales décisions quant aux finalités, aux conditions et aux moyens du traitement de données à caractère personnel; si aucune décision de ce type n'est prise dans l'Union, l'établissement principal est le lieu où sont exercées les principales activités de traitement dans le cadre des activités d'un établissement d'un responsable du traitement dans l'Union; en ce qui concerne le sous-traitant, on entend par «établissement principal» le lieu de son administration centrale dans l'Union;

(14) «représentant»: toute personne physique ou morale établie dans l'Union expressément désignée par le responsable du traitement, qui agit en lieu et place de ce dernier et peut être contactée à sa place par les autorités de contrôle et d'autres entités dans l'Union, en ce qui concerne les obligations du responsable du traitement en vertu du présent règlement;

(15) «entreprise»: toute entité exerçant une activité économique, quelle que soit sa forme juridique, y compris, notamment, les personnes physiques et morales, les sociétés de personnes ou les associations qui exercent régulièrement une activité économique;

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

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

(18) «enfant»: toute personne âgée de moins de dix-huit ans;

(19) «autorité de contrôle»: une autorité publique qui est instituée par un État membre conformément aux dispositions de l'article 46.

CHAPITRE II
PRINCIPES

Article 5
Principes relatifs au traitement des données à caractère personnel

Les données à caractère personnel doivent être:

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

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités;

c) adéquates, pertinentes et limitées au minimum nécessaire au regard des finalités pour lesquelles elles sont traitées; elles ne sont traitées que si, et pour autant que, les finalités du traitement ne peuvent pas être atteintes par le traitement d'informations ne contenant pas de données à caractère personnel;

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

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles ne seront traitées qu'à des fins de recherche historique, statistique ou scientifique conformément aux règles et aux conditions énoncées à l'article 83 et s'il est procédé à un examen périodique visant à évaluer la nécessité de poursuivre la conservation;

f) traitées sous la responsabilité du responsable du traitement, qui veille à la conformité de chaque opération de traitement avec les dispositions du présent règlement et en apporte la preuve .

Article 6
Licéité du traitement

1. Le traitement de données à caractère personnel n'est licite que si et dans la mesure où l'une au moins des situations suivantes s'applique:

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;

e) le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt général 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 un responsable du traitement, 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. Ces considérations ne s'appliquent pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

2. Le traitement de données à caractère personnel qui est nécessaire à des fins de recherche historique, statistique ou scientifique est licite sous réserve des conditions et des garanties prévues à l'article 83.

3. Le fondement juridique du traitement visé au paragraphe 1, points c) et e), doit être prévu dans:

a) le droit de l'Union, ou

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

La législation de l'État membre doit répondre à un objectif d'intérêt général ou être nécessaire à la protection des droits et libertés d'autrui, être respectueuse du contenu essentiel du droit à la protection des données à caractère personnel et proportionnée à l'objectif légitime poursuivi.

4. Lorsque la finalité du traitement ultérieur n'est pas compatible avec celle pour laquelle les données à caractère personnel ont été collectées le traitement doit trouver sa base juridique au moins dans l'un des motifs mentionnés au paragraphe 1, points a) à e). Ceci s'applique en particulier à toute modification des clauses et des conditions générales d'un contrat.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les conditions prévues au paragraphe 1, point f), pour divers secteurs et situations en matière de traitement de données, y compris en ce qui concerne le traitement des données à caractère personnel relatives à un enfant.

Article 7

Conditions de consentement

1. La charge de prouver que la personne concernée a consenti au traitement de ses données à caractère personnel à des fins déterminées incombe au responsable du traitement.

2. Si le consentement de la personne concernée est requis dans le contexte d'une déclaration écrite qui concerne également une autre affaire, l'exigence du consentement doit apparaître sous une forme qui le distingue de cette autre affaire.

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

4. Le consentement ne constitue pas un fondement juridique valable pour le traitement lorsqu'il existe un déséquilibre significatif entre la personne concernée et le responsable du traitement.

Article 8

Traitement de données à caractère personnel relatives aux enfants

1. Aux fins du présent règlement, s'agissant de l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant de moins de 13 ans n'est licite que si et dans la mesure où le consentement est donné ou autorisé par un parent de l'enfant ou par une personne qui en a la garde. Le responsable du traitement s'efforce raisonnablement d'obtenir un consentement vérifiable, compte tenu des moyens techniques disponibles.

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

3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables aux méthodes d'obtention du consentement vérifiable visé au paragraphe 1. Ce faisant, la Commission envisage des mesures spécifiques pour les micro, petites et moyennes entreprises.

4. La Commission peut établir des formulaires types pour les méthodes particulières d'obtention du consentement vérifiable prévu au paragraphe 1. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Article 9

Traitements portant sur des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances, l'appartenance syndicale, ainsi que le traitement des données génétiques ou des données concernant

la santé ou relatives à la vie sexuelle ou à des condamnations pénales ou encore à des mesures de sûreté connexes sont interdits.

2. Le paragraphe 1 ne s'applique pas lorsque:

a) la personne concernée a donné son consentement au traitement de ces données à caractère personnel, dans les conditions fixées à l'article 7 et à l'article 8, sauf lorsque le droit de l'Union ou la législation nationale prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée; ou

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement en matière de droit du travail, dans la mesure où ce traitement est autorisé par le droit de l'Union ou par une législation nationale prévoyant des garanties appropriées; ou

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

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

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

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice; ou

g) le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt général sur le fondement du droit de l'Union ou d'un État membre, qui doit prévoir des mesures appropriées à la sauvegarde des intérêts légitimes de la personne concernée; ou

h) le traitement des données relatives à la santé est nécessaire à des fins liées à la santé, sous réserve des conditions et des garanties prévues à l'article 81; ou

i) le traitement est nécessaire à des fins de recherche historique, statistique ou scientifique, sous réserve des conditions et des garanties prévues à l'article 83; ou

j) le traitement des données relatives aux condamnations pénales ou aux mesures de sûreté connexes est effectué soit sous le contrôle de l'autorité publique, ou lorsque le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis, ou à l'exécution d'une mission effectuée pour des motifs importants d'intérêt général, dans la mesure où ce traitement est autorisé par le droit de l'Union ou

par la législation d'un État membre prévoyant des garanties adéquates. Un registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

3. La Commission est habilitée à adopter des actes délégués en conformité avec l’article 86, aux fins de préciser davantage les critères, les conditions et les garanties appropriées pour le traitement des catégories particulières de données à caractère personnel mentionnées au paragraphe 1, ainsi que les dérogations prévues au paragraphe 2.

Article 10
Traitement ne permettant pas l'identification

Si les données traitées par un responsable du traitement ne lui permettent pas d'identifier une personne physique, le responsable du traitement n'est pas tenu d'obtenir des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter une disposition du présent règlement.

CHAPITRE III
DROITS DE LA PERSONNE CONCERNÉE

SECTION 1
TRANSPARENCE ET MODALITÉS

Article 11
Transparence des informations et des communications

1. Le responsable du traitement applique des règles internes transparentes et facilement accessibles en ce qui concerne le traitement des données à caractère personnel et en vue de l’exercice de leurs droits par les personnes concernées.

2. Le responsable du traitement procède à toutes information et communication relatives au traitement des données à caractère personnel à la personne concernée, sous une forme intelligible et en des termes clairs et simples, adaptés à la personne concernée, en particulier lorsqu'une information est adressée spécifiquement à un enfant.

Article 12
Procédures et mécanismes prévus pour l'exercice des droits de la personne concernée

1. Le responsable du traitement établit les procédures d'information prévues à l’article 14 et les procédures d'exercice des droits des personnes concernées mentionnés aux articles 13, et 15 à 19. Il met notamment en place des mécanismes facilitant l’introduction de la demande portant sur les mesures prévues aux articles 13, et 15 à 19. Lorsque des données à caractère personnel font l'objet d'un traitement automatisé, le responsable du traitement doit également fournir les moyens d'effectuer des demandes par voie électronique.

2. Le responsable du traitement informe la personne concernée sans tarder et, au plus tard, dans un délai d'un mois à compter de la réception de la demande, indépendamment de l'éventuelle adoption d'une mesure conformément aux articles 13, et 15 à 19 et fournit les informations demandées. Ce délai peut être prolongé d'un mois, si plusieurs personnes concernées exercent leurs droits et si leur coopération est suffisamment nécessaire pour empêcher un effort inutile et disproportionné de la part du responsable du traitement. Ces informations sont données par écrit. Lorsque la personne concernée en fait la demande sous forme électronique, les informations sont fournies sous forme électronique, à moins que la personne concernée ne demande qu'il en soit autrement.

3. Si le responsable du traitement refuse de prendre des mesures demandées par la personne concernée, il informe cette dernière des motifs du refus, des possibilités d'introduire une réclamation auprès de l'autorité de contrôle et de former un recours juridictionnel.

4. Les informations et les mesures prises dans le cadre des demandes visées au paragraphe 1 sont gratuites. Lorsque les demandes sont manifestement excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut exiger le paiement de frais pour fournir les informations ou pour prendre les mesures demandées, peut s'abstenir de prendre les mesures demandées. Dans ce cas, il incombe au responsable du traitement de prouver le caractère manifestement excessif de la demande.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et conditions applicables aux demandes manifestement excessives, et les frais visés au paragraphe 4.

6. La Commission peut établir des formulaires types et préciser des procédures types pour la communication visée au paragraphe 2, y compris sous forme électronique. Ce faisant, la Commission prend les mesures appropriées pour les micro, petites et moyennes entreprises. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Article 13
Droits à l'égard des destinataires

Le responsable du traitement communique à chaque destinataire à qui les données ont été transmises toute rectification ou effacement effectué conformément aux articles 16 et 17, à moins qu'une telle communication se révèle impossible ou suppose un effort disproportionné.

SECTION 2
INFORMATION ET ACCÈS AUX DONNÉES

Article 14
Informations à fournir la personne concernée

1. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées, le responsable du traitement doit fournir à cette personne au moins les informations suivantes:

a) l’identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable et celles du délégué à la protection des données;

b) les finalités du traitement auquel sont destinées les données à caractère personnel, y compris les clauses et les conditions générales du contrat lorsque le traitement est fondé sur l’article 6, paragraphe 1, point b), et les intérêts légitimes poursuivis par le responsable du traitement lorsque le traitement est fondé sur l’article 6, paragraphe 1, point f);

c) la durée pendant laquelle les données à caractère personnel seront conservées;

d) l’existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel relatives à la personne concernée, la rectification ou l'effacement de celles-ci, ou du droit de s'opposer au traitement de ces données;

e) le droit d’introduire une réclamation auprès de l'autorité de contrôle et les coordonnées de ladite autorité;

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

g) le cas échéant, son intention d'effectuer un transfert vers un pays tiers ou à une organisation internationale, et le niveau de protection offert par le pays tiers ou l'organisation internationale en question, par référence à une décision relative au caractère adéquat du niveau de protection rendue par la Commission;

h) toute autre information nécessaire pour assurer un traitement loyal des données à l'égard de la personne concernée, compte tenu des circonstances particulières dans lesquelles les données à caractère personnel sont collectées.

2. Lorsque les données à caractère personnel sont collectées auprès de la personne concernée, le responsable du traitement fournit à cette dernière, outre les informations mentionnées au paragraphe 1, des informations sur le caractère obligatoire ou facultatif de la fourniture des données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données.

3. Lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, le responsable du traitement fournit à cette dernière, outre les informations mentionnées au paragraphe 1, des informations relatives à l'origine des données à caractère personnel.

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

a) au moment où les données à caractère personnel sont recueillies auprès de la personne concernée, ou

b) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, au moment de l’enregistrement ou dans un délai raisonnable après la collecte, eu égard aux circonstances particulières dans lesquelles les données sont collectées ou traitées, ou si la communication à un

autre destinataire est envisagée, et au plus tard au moment où les données sont communiquées pour la première fois.

5. Les dispositions des paragraphes 1 et 4 ne s'appliquent pas lorsque:

a) la personne concernée dispose déjà des informations visées aux paragraphes 1, 2 et 3; ou

b) les données ne sont pas collectées auprès de la personne concernée et que la fourniture de ces informations se révèle impossible ou supposerait des efforts disproportionnés; ou

c) les données ne sont pas collectées auprès de la personne concernée et que l'enregistrement ou la communication des données sont expressément prévus par la législation; ou

d) les données ne sont pas collectées auprès de la personne concernée et que la fourniture de ces informations porte atteinte aux droits et libertés d'autrui tels qu'ils sont définis dans le droit de l'Union ou le droit des États membres, conformément à l'article 21.

6. Dans le cas visé au paragraphe 5, point b), le responsable du traitement prend les mesures appropriées pour protéger les intérêts légitimes de la personne concernée.

7. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères applicables aux catégories de destinataires visées au paragraphe 1, point f), l'obligation d'informer sur les possibilités d'accès prévues au paragraphe 1, point g), les critères applicables à l'obtention des informations supplémentaires nécessaires visées au paragraphe 1, point h), pour les secteurs et les situations spécifiques, et les conditions et les garanties appropriées encadrant les exceptions prévues au paragraphe 5, point b). Ce faisant, la Commission prend les mesures appropriées pour les micro, petites et moyennes entreprises.

8. La Commission peut établir des formulaires types pour la communication des informations énumérées aux paragraphes 1 à 3, compte tenu des caractéristiques et des besoins particuliers des différents secteurs et, le cas échéant, des situations impliquant le traitement de données. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Article 15
Droit d'accès de la personne concernée

1. La personne concernée a le droit d'obtenir, à tout moment, à sa demande, auprès du responsable du traitement, confirmation que les données à caractère personnel la concernant sont ou ne sont pas traitées. Lorsque ces données à caractère personnel sont traitées, le responsable du traitement fournit les informations suivantes:

a) les finalités du traitement;

b) les catégories de données à caractère personnel concernées;

c) les destinataires ou les catégories de destinataires auxquels les données à caractère personnel doivent être ou ont été communiquées, en particulier lorsque les destinataires sont établis dans des pays tiers;

d) la durée pendant laquelle les données à caractère personnel seront conservées;

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

f) le droit d'introduire une réclamation auprès de l'autorité de contrôle et les coordonnées de ladite autorité;

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

h) l'importance et les conséquences envisagées de ce traitement, au moins dans le cas des mesures prévues à l'article 20.

2. La personne concernée a le droit d'obtenir du responsable du traitement la communication des données à caractère personnel en cours de traitement. Lorsque la personne concernée en fait la demande sous forme électronique, les informations sont fournies sous forme électronique, à moins que la personne concernée ne demande qu'il en soit autrement.

3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables à la communication, à la personne concernée, du contenu des données à caractère personnel mentionnées au paragraphe 1, point g).

4. La Commission peut préciser les formulaires types et les procédures de demande et d'accès aux informations mentionnées au paragraphe 1, y compris pour la vérification de l'identité de la personne concernée et la communication de ses données à caractère personnel à la personne concernée, compte tenu des besoins et des caractéristiques spécifiques des différents secteurs et situations impliquant le traitement de données. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

SECTION 3

RECTIFICATION ET EFFACEMENT

Article 16

Droit de rectification

La personne concernée a le droit d'obtenir du responsable du traitement la rectification des données à caractère personnel la concernant qui sont inexactes. La personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris au moyen d'une déclaration rectificative complémentaire.

Article 17

Droit à l'oubli numérique et à l'effacement

1. La personne concernée a le droit d'obtenir du responsable du traitement l’effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données, en particulier en ce qui concerne des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu’elle était enfant, ou pour l'un des motifs suivants:

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

   b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données;

   c) la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19;

   d) le traitement des données n'est pas conforme au présent règlement pour d'autres motifs.

2. Lorsque le responsable du traitement visé au paragraphe 1 a rendu publiques les données à caractère personnel, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci. Lorsque le responsable du traitement a autorisé un tiers à publier des données à caractère personnel, il est réputé responsable de cette publication.

3. Le responsable du traitement procède à l'effacement sans délai, sauf lorsque la conservation des données à caractère personnel est nécessaire:

   a) à l'exercice du droit à la liberté d'expression, conformément à l'article 80;

   b) pour des motifs d'intérêt général dans le domaine de la santé publique, conformément à l'article 81;

   c) à des fins de recherche historique, statistique et scientifique, conformément à l'article 83;

   d) au respect d'une obligation légale de conserver les données à caractère personnel prévue par le droit de l'Union ou par la législation d'un État membre à laquelle le responsable du traitement est soumis; la législation de l'État membre doit répondre à un objectif d’intérêt général, respecter le contenu essentiel du droit à la protection des données à caractère personnel et être proportionnée à l'objectif légitime poursuivi;

   e) dans les cas mentionnés au paragraphe 4.

4. Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement de données à caractère personnel:

a) pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données lorsque cette dernière est contestée par la personne concernée;

b) lorsqu'elles ne sont plus utiles au responsable du traitement pour qu'il s'acquitte de sa mission, mais qu'elles doivent être conservées à des fins probatoires, ou

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

d) lorsque la personne concernée demande le transfert des données à caractère personnel à un autre système de traitement automatisé, conformément à l'article 18, paragraphe 2.

5. Les données à caractère personnel énumérées au paragraphe 4 ne peuvent être traitées, à l'exception de la conservation, qu'à des fins probatoires, ou avec le consentement de la personne concernée, ou aux fins de la protection des droits d'une autre personne physique ou morale ou pour un objectif d'intérêt général.

6. Lorsque le traitement des données à caractère personnel est limité conformément au paragraphe 4, le responsable du traitement informe la personne concernée avant de lever la limitation frappant le traitement.

7. Le responsable du traitement met en œuvre des mécanismes assurant le respect des délais applicables à l'effacement des données à caractère personnel et/ou à un examen périodique de la nécessité de conserver ces données.

8. Lorsque l'effacement est effectué, le responsable du traitement ne procède à aucun autre traitement de ces données à caractère personnel.

9. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser:

a) les exigences et critères relatifs à l'application du paragraphe 1 dans des secteurs spécifiques et des situations spécifiques impliquant le traitement de données;

b) les conditions de la suppression des liens vers ces 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 le paragraphe 2;

c) les conditions et critères applicables à la limitation du traitement des données à caractère personnel, visés au paragraphe 4.

Article 18
Droit à la portabilité des données

1. Lorsque des données à caractère personnel font l'objet d'un traitement automatisé dans un format structuré et couramment utilisé, la personne concernée a le droit d'obtenir auprès du responsable du traitement une copie des données faisant l'objet du traitement automatisé dans un format électronique structuré qui est couramment utilisé et qui permet la réutilisation de ces données par la personne concernée.

2. Lorsque la personne concernée a fourni les données à caractère personnel et que le traitement est fondé sur le consentement ou sur un contrat, elle a le droit de transmettre ces données à caractère personnel et toutes autres informations qu'elle a fournies et qui sont conservées par un système de traitement automatisé à un autre système dans un format électronique qui est couramment utilisé, sans que le responsable du traitement auquel les données à caractère personnel sont retirées n'y fasse obstacle.

3. La Commission peut préciser le format électronique visé au paragraphe 1, ainsi que les normes techniques, les modalités et les procédures pour la transmission de données à caractère personnel conformément au paragraphe 2. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

SECTION 4
DROIT D'OPPOSITION ET PROFILAGE

Article 19
Droit d'opposition

1. La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à ce que des données à caractère personnel fassent l'objet d'un traitement fondé sur l'article 6, paragraphe 1, points d), e) et f), à moins que le responsable du traitement n'établisse l’existence de raisons impérieuses et légitimes justifiant le traitement, qui priment les intérêts ou les libertés et droits fondamentaux de la personne concernée.

2. Lorsque les données à caractère personnel sont traitées à des fins de marketing direct, la personne concernée a le droit de s'opposer au traitement de ses données à caractère personnel en vue de ce marketing direct. Ce droit est explicitement proposé à la personne concernée d'une façon intelligible et doit pouvoir être clairement distingué d'autres informations.

3. Lorsqu'il est fait droit à une opposition conformément aux paragraphes 1 et 2, le responsable du traitement n'utilise ni ne traite plus les données à caractère personnel concernées.

Article 20
Mesures fondées sur le profilage

1. Toute personne physique a le droit de ne pas être soumise à une mesure produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects personnels propres à cette personne physique ou à analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement.

2. Sous réserve des autres dispositions du présent règlement, une personne ne peut être soumise à une mesure telle que celle visée au paragraphe 1 que si le traitement:

   a) est effectué dans le cadre de la conclusion ou de l'exécution d'un contrat, lorsque la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, a été satisfaite ou qu'ont été invoquées des mesures appropriées garantissant la sauvegarde des intérêts légitimes de la personne concernée, tels que le droit d'obtenir une intervention humaine; ou

   b) est expressément autorisé par une législation de l'Union ou d'un État membre qui prévoit également des mesures appropriées garantissant la sauvegarde des intérêts légitimes de la personne concernée; ou

   c) est fondé sur le consentement de la personne concernée, sous réserve des conditions énoncées à l'article 7 et de garanties appropriées.

3. Le traitement automatisé de données à caractère personnel destiné à évaluer certains aspects personnels propres à une personne physique ne saurait être exclusivement fondé sur les catégories particulières de données à caractère personnel mentionnées à l'article 9.

4. Dans les cas prévus au paragraphe 2, les informations que le responsable du traitement doit fournir en vertu de l'article 14 comportent notamment des informations relatives à l'existence du traitement pour une mesure telle que celle visée au paragraphe 1 et aux effets escomptés de ce traitement sur la personne concernée.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et conditions applicables aux mesures appropriées garantissant la sauvegarde des intérêts légitimes de la personne concernée conformément au paragraphe 2.

SECTION 5
LIMITATIONS

Article 21
Limitations

1. Le droit de l'Union ou le droit des États membres peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus à l'article 5,

points a) à e), aux articles 11 à 20 et à l'article 32, lorsqu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour:

a) assurer la sécurité publique;

b) assurer la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière;

c) sauvegarder d'autres intérêts généraux 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, ainsi que la stabilité et l'intégrité des marchés;

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

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

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

2. Tout mesure législative visée au paragraphe 1 doit notamment contenir des dispositions spécifiques relatives, au moins, aux finalités du traitement et aux modalités d'identification du responsable du traitement.

CHAPITRE IV

RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT

SECTION 1
OBLIGATIONS GÉNÉRALES

Article 22

Obligations incombant au responsable du traitement

1. Le responsable du traitement adopte des règles internes et met en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du présent règlement.

2. Les mesures prévues au paragraphe 1 portent notamment sur:

a) la tenue de la documentation en application de l'article 28;

b) la mise en œuvre des obligations en matière de sécurité des données prévues à l'article 30;

c) la réalisation d'une analyse d'impact relative à la protection des données en application de l'article 33;

d) le respect des obligations en matière d'autorisation ou de consultation préalables de l'autorité de contrôle en application de l'article 34, paragraphes 1 et 2;

e) la désignation d'un délégué à la protection des données en application de l'article 35, paragraphe 1.

3. Le responsable du traitement met en œuvre des mécanismes pour vérifier l'efficacité des mesures énoncées aux paragraphes 1 et 2. Sous réserve de la proportionnalité d'une telle mesure, des auditeurs indépendants internes ou externes procèdent à cette vérification.

4. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage d'éventuels critères et exigences supplémentaires applicables aux mesures appropriées visées au paragraphe 1, autres que celles déjà visés au paragraphe 2, les conditions de vérification et mécanismes d'audit visés au paragraphe 3 et le critère de proportionnalité prévu au paragraphe 3, et afin d'envisager des mesures spécifiques pour les micro, petites entreprises et moyennes entreprises.

Article 23

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

1. Compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, le responsable du traitement applique, tant lors de la définition des moyens de traitement que lors du traitement proprement dit, les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée.

2. Le responsable du traitement met en œuvre des mécanismes visant à garantir que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées ou conservées au-delà du minimum nécessaire à ces finalités, pour ce qui est tant de la quantité de données que de la durée de leur conservation. En particulier, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques.

3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser d'éventuels critères et exigences supplémentaires applicables aux mesures appropriées et aux mécanismes visés aux paragraphes 1 et 2, en ce qui concerne notamment les exigences en matière de protection des données dès la conception applicables à l'ensemble des secteurs, produits et services.

4. La Commission peut définir des normes techniques pour les exigences fixées aux paragraphes 1 et 2. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Article 24

Responsables conjoints du traitement

Lorsqu'un responsable du traitement définit, conjointement avec d'autres, les finalités, conditions et moyens du traitement de données à caractère personnel, les responsables conjoints du traitement définissent, par voie d'accord, leurs obligations respectives afin de se conformer aux exigences du présent règlement, en ce qui concerne notamment les procédures et mécanismes régissant l'exercice des droits de la personne concernée.

Article 25

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

1. Dans le cas visé à l'article 3, paragraphe 2, le responsable du traitement désigne un représentant dans l'Union.

2. Cette obligation ne s'applique pas:

   a) à un responsable du traitement établi dans un pays tiers lorsque la Commission a constaté par voie de décision que ce pays tiers assurait un niveau de protection adéquat conformément à l'article 41; ou

   b) à une entreprise employant moins de 250 salariés; ou

   c) à une autorité ou à un organisme publics; ou

   d) à un responsable du traitement n'offrant qu'occasionnellement des biens ou des services à des personnes concernées résidant dans l'Union.

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

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

Article 26

Sous-traitant

1. Lorsque le traitement est effectué pour son compte, le responsable du traitement choisit un sous-traitant qui présente des garanties suffisantes de mise en œuvre des mesures et procédures techniques et organisationnelles appropriées, de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée, en ce qui concerne notamment les mesures de sécurité technique et d'organisation régissant le traitement à effectuer, et veille au respect de ces mesures.

2. La réalisation de traitements en sous-traitance est régie par un contrat ou un autre acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant:

a) n'agit que sur instruction du responsable du traitement, en particulier lorsque le transfert des données à caractère personnel utilisées est interdit;

b) n'emploie que du personnel qui a pris des engagements de confidentialité ou qui est soumis à une obligation légale de confidentialité;

c) prend toutes les mesures nécessaires en vertu de l'article 30;

d) n'engage un autre sous-traitant que moyennant l'autorisation préalable du responsable du traitement;

e) dans la mesure du possible compte tenu de la nature du traitement, crée, en accord avec le responsable du traitement, les conditions techniques et organisationnelles nécessaires pour permettre au responsable du traitement de 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 30 à 34;

g) transmet tous les résultats au responsable du traitement après la fin du traitement et s'abstient de traiter les données à caractère personnel de toute autre manière;

h) met à la disposition du responsable du traitement et de l'autorité de contrôle toutes les informations nécessaires au contrôle du respect des obligations prévues par le présent article.

3. Le responsable du traitement et le sous-traitant conservent une trace documentaire des instructions données par le responsable du traitement et des obligations du sous-traitant énoncées au paragraphe 2.

4. S'il traite des données à caractère personnel d'une manière autre que celle définie dans les instructions du responsable du traitement, le sous-traitant est considéré comme responsable du traitement à l'égard de ce traitement et il est soumis aux dispositions applicables aux responsables conjoints du traitement prévues à l'article 24.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables aux responsabilités, obligations et missions d'un sous-traitant en conformité avec le paragraphe 1, ainsi que les conditions qui permettent de faciliter le traitement des données à caractère personnel au sein d'un groupe d'entreprises, en particulier aux fins de contrôle et de présentation de rapports.

Article 27

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

Le sous-traitant ainsi que toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, à moins d'y être obligé par la législation de l'Union ou d'un État membre.

Article 28

Documentation

1. Chaque responsable du traitement et chaque sous-traitant ainsi que, le cas échéant, le représentant du responsable du traitement, conservent une trace documentaire de tous les traitements effectués sous leur responsabilité.

2. La documentation constituée comporte au moins les informations suivantes:

   a) le nom et les coordonnées du responsable du traitement, ou de tout responsable conjoint du traitement ou de tout sous-traitant, et du représentant, le cas échéant;

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

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

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

   e) les destinataires ou les catégories de destinataires des données à caractère personnel, y compris les responsables du traitement auxquels les données à caractère personnel sont communiquées aux fins de l'intérêt légitime qu'ils poursuivent;

   f) le cas échéant, les transferts de données vers un pays tiers ou à une organisation internationale, y compris le nom de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 44, paragraphe 1, point h), les documents attestant l'existence de garanties appropriées;

   g) une indication générale des délais impartis pour l'effacement des différentes catégories de données;

   h) la description des mécanismes prévus à l'article 22, paragraphe 3.

3. Le responsable du traitement et le sous-traitant ainsi que, le cas échéant, le représentant du responsable du traitement mettent la documentation à la disposition de l'autorité de contrôle, à la demande de celle-ci.

4. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas aux responsables du traitement et aux sous-traitants relevant des catégories suivantes:

a) personnes physiques traitant des données à caractère personnel en l'absence de tout intérêt commercial; ou

b) entreprises ou organismes comptant moins de 250 salariés traitant des données à caractère personnel uniquement dans le cadre d'une activité qui est accessoire à leur activité principale.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables à la documentation visée au paragraphe 1, pour tenir compte, notamment, des obligations du responsable du traitement et du sous-traitant et, le cas échéant, du représentant du responsable du traitement.

6. La Commission peut établir des formulaires types pour la documentation visée au paragraphe 1. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Article 29
Coopération avec l'autorité de contrôle

1. Le responsable du traitement et le sous-traitant ainsi que, le cas échéant, le représentant du responsable du traitement, coopèrent, sur demande, avec l'autorité de contrôle dans l'exécution de ses fonctions, en communiquant notamment les informations énoncées à l'article 53, paragraphe 2, point a), et en accordant un accès, conformément aux dispositions du point b) dudit paragraphe.

2. Lorsque l'autorité de contrôle exerce les pouvoirs qui lui sont conférés en vertu de l'article 53, paragraphe 2, le responsable du traitement et le sous-traitant répondent à l'autorité de contrôle dans un délai raisonnable devant être fixé par celle-ci. La réponse comprend une description des mesures prises et des résultats obtenus, compte tenu des observations formulées par l'autorité de contrôle.

SECTION 2
SÉCURITÉ DES DONNÉES

Article 30
Sécurité des traitements

1. Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir, compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, un niveau de sécurité adapté aux risques présentés par le traitement et à la nature des données à caractère personnel à protéger.

2. À la suite d'une évaluation des risques, le responsable du traitement et le sous-traitant prennent les mesures prévues au paragraphe 1 pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite et la perte accidentelle et pour

empêcher toute forme illicite de traitement, notamment la divulgation, la diffusion ou l'accès non autorisés, ou l'altération de données à caractère personnel.

3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables aux mesures techniques et d'organisation visées aux paragraphes 1 et 2, y compris le point de savoir quelles sont les techniques les plus modernes, pour des secteurs spécifiques et dans des cas spécifiques de traitement de données, notamment compte tenu de l'évolution des techniques et des solutions de protection des données dès la conception ainsi que par défaut, sauf si le paragraphe 4 s'applique.

4. La Commission peut adopter, le cas échéant, des actes d'exécution afin de préciser les exigences prévues aux paragraphes 1 et 2 dans diverses situations, en particulier en vue:

   a) d'empêcher tout accès non autorisé à des données à caractère personnel;

   b) d'empêcher toute forme non autorisée de divulgation, de lecture, de copie, de modification, d'effacement ou de suppression de données à caractère personnel;

   c) d'assurer la vérification de la licéité des traitements.

   Ces actes d'exécution sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Article 31

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

1. En cas de violation de données à caractère personnel, le responsable du traitement en adresse notification à l'autorité de contrôle sans retard injustifié et, si possible, 24 heures au plus tard après en avoir pris connaissance. Lorsqu'elle a lieu après ce délai de 24 heures, la notification comporte une justification à cet égard.

2. En vertu de l'article 26, paragraphe 2, point f), le sous-traitant alerte et informe le responsable du traitement immédiatement après avoir constaté la violation de données à caractère personnel.

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 les catégories et le nombre de personnes concernées par la violation et les catégories et le nombre d'enregistrements de données concernés;

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

   c) recommander des mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données à caractère personnel;

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

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

4. Le responsable du traitement conserve une trace documentaire de toute violation de données à caractère personnel, en indiquant son contexte, ses effets et les mesures prises pour y remédier. La documentation constituée doit permettre à l'autorité de contrôle de vérifier le respect des dispositions du présent article. Elle comporte uniquement les informations nécessaires à cette fin.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables à l'établissement de la violation de données visée aux paragraphes 1 et 2 et concernant les circonstances particulières dans lesquelles un responsable du traitement et un sous-traitant sont tenus de notifier la violation de données à caractère personnel.

6. La Commission peut définir la forme normalisée de cette notification à l'autorité de contrôle, les procédures applicables à l'obligation de notification ainsi que le formulaire type et les modalités selon lesquelles est constituée la documentation visée au paragraphe 4, y compris les délais impartis pour l'effacement des informations qui y figurent. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Article 32

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

1. Lorsque la violation de données à caractère personnel est susceptible de porter atteinte à la protection des données à caractère personnel ou à la vie privée de la personne concernée, le responsable du traitement, après avoir procédé à la notification prévue à l'article 31, communique la violation sans retard indu à la personne concernée.

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

3. La communication à la personne concernée d'une violation de ses données à caractère personnel n'est pas nécessaire si le responsable du traitement prouve, à la satisfaction de l'autorité de contrôle, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques doivent rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

4. Sans préjudice de l'obligation du responsable du traitement de communiquer à la personne concernée la violation de ses données à caractère personnel, si le responsable du traitement n'a pas déjà averti la personne concernée de la violation de ses données à caractère personnel, l'autorité de contrôle peut, après avoir examiné les effets potentiellement négatifs de cette violation, exiger du responsable du traitement qu'il s'exécute.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences concernant les circonstances, visées au paragraphe 1, dans lesquelles une violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personnel.

6. La Commission peut définir la forme de la communication à la personne concernée prévue au paragraphe 1 et les procédures applicables à cette communication. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

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

Article 33
Analyse d'impact relative à la protection des données

1. Lorsque les traitements présentent des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités, le responsable du traitement ou le sous-traitant agissant pour le compte du responsable du traitement effectuent une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel.

2. Les traitements présentant les risques particuliers visés au paragraphe 1 sont notamment les suivants:

   a) l'évaluation systématique et à grande échelle des aspects personnels propres à une personne physique ou visant à analyser ou à prévoir, en particulier, la situation économique de ladite personne physique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement, qui est fondée sur un traitement automatisé et sur la base de laquelle sont prises des mesures produisant des effets juridiques concernant ou affectant de manière significative ladite personne;

   b) le traitement d'informations relatives à la vie sexuelle, à la santé, à l'origine raciale et ethnique ou destinées à la fourniture de soins de santé, à des recherches épidémiologiques ou à des études relatives à des maladies mentales ou infectieuses, lorsque les données sont traitées aux fins de l'adoption de mesures ou de décisions à grande échelle visant des personnes précises;

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

   d) le traitement de données à caractère personnel dans des fichiers informatisés de grande ampleur concernant des enfants, ou le traitement de données génétiques ou biométriques;

   e) les autres traitements pour lesquels la consultation de l'autorité de contrôle est requise en application à l'article 34, paragraphe 2, point b).

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

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

5. Lorsque le responsable du traitement est une autorité ou un organisme publics, et lorsque le traitement est effectué en exécution d'une obligation légale conforme à l'article 6, paragraphe 1, point c), prévoyant des règles et des procédures relatives aux traitements et réglementées par le droit de l'Union, les paragraphes 1 à 4 ne s'appliquent pas, sauf si les États membres estiment qu'une telle analyse est nécessaire avant le traitement.

6. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et conditions applicables aux traitements susceptibles de présenter les risques particuliers visés aux paragraphes 1 et 2, ainsi que les exigences applicables à l'analyse prévue au paragraphe 3, y compris les conditions de modularité, de vérification et d'auditabilité. Ce faisant, la Commission envisage des mesures spécifiques pour les micro, petites et moyennes entreprises.

7. La Commission peut définir des normes et procédures pour la réalisation, la vérification et l'audit de l'analyse visée au paragraphe 3. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Article 34
Autorisation et consultation préalables

1. Le responsable du traitement ou le sous-traitant, selon le cas, obtiennent une autorisation de l'autorité de contrôle avant le traitement de données à caractère personnel afin de garantir la conformité du traitement prévu avec le présent règlement et, notamment, d'atténuer les risques pour les personnes concernées lorsqu'un responsable du traitement ou un sous-traitant adoptent des clauses contractuelles telles que celles prévues à l'article 42, paragraphe 2, point d), ou n'offrent pas les garanties appropriées dans un instrument juridiquement contraignant tel que visé à l'article 42, paragraphe 5, régissant le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale.

2. Le responsable du traitement ou le sous-traitant agissant au nom du responsable du traitement consultent l'autorité de contrôle avant le traitement de données à caractère personnel afin de garantir la conformité du traitement prévu avec le présent règlement et, notamment, d'atténuer les risques pour les personnes concernées:

a) lorsqu'une analyse d'impact relative à la protection des données telle que prévue à l'article 33 indique que les traitements sont, du fait de leur nature, de leur portée ou de leurs finalités, susceptibles de présenter un degré élevé de risques particuliers; ou

b) lorsque l'autorité de contrôle estime nécessaire de procéder à une consultation préalable au sujet de traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, du fait de leur nature, de leur portée et/ou de leurs finalités, ces traitements étant précisés conformément au paragraphe 4.

3. Lorsque l'autorité de contrôle est d'avis que le traitement prévu n'est pas conforme au présent règlement, en particulier lorsque les risques ne sont pas suffisamment identifiés ou atténués, elle interdit le traitement prévu et formule des propositions appropriées afin de remédier à cette non-conformité.

4. L'autorité de contrôle établit et publie une liste des traitements devant faire l'objet d'une consultation préalable au titre du paragraphe 2, point b). L'autorité de contrôle communique cette liste au comité européen de la protection des données.

5. Si la liste prévue au paragraphe 4 comprend des traitements liés à l'offre de biens ou de services à des personnes concernées dans plusieurs États membres ou liés à l'observation de leur comportement, ou susceptibles d'affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union, l'autorité de contrôle applique le mécanisme de contrôle de la cohérence prévu à l'article 57 avant d'adopter la liste.

6. Le responsable du traitement ou le sous-traitant fournissent à l'autorité de contrôle l'analyse d'impact relative à la protection des données prévue à l'article 33 et, sur demande, toute autre information afin de permettre à l'autorité de contrôle d'apprécier la conformité du traitement et, en particulier, les risques pour la protection des données à caractère personnel de la personne concernée et les garanties qui s'y rapportent.

7. Les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une mesure législative devant être adoptée par le parlement national ou d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement, en vue d'assurer la conformité du traitement prévu avec le présent règlement et, en particulier, d'atténuer les risques pour les personnes concernées.

8. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables à la détermination du niveau élevé de risque particulier visé au paragraphe 2, point a).

9. La Commission peut élaborer des formulaires et procédures types pour les autorisations et consultations préalables visées aux paragraphes 1 et 2, ainsi que des formulaires et procédures types pour l'information des autorités de contrôle au titre du paragraphe 6. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

SECTION 4
DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Article 35
Désignation du délégué à la protection des données

1. Le responsable du traitement et le sous-traitant désignent systématiquement un délégué à la protection des données lorsque:

   a) le traitement est effectué par une autorité ou un organisme publics; ou

   b) le traitement est effectué par une entreprise employant 250 personnes ou plus; ou

   c) les activités de base du responsable du traitement ou du sous-traitant consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées.

2. Dans le cas visé au paragraphe 1, point b), un groupe d'entreprises peut désigner un délégué à la protection des données unique.

3. Lorsque le responsable du traitement ou le sous-traitant est une autorité ou un organisme publics, le délégué à la protection des données peut être désigné pour plusieurs de ses entités, compte tenu de la structure organisationnelle de l'autorité ou de l'organisme publics.

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 un délégué à la protection des données.

5. Le responsable du traitement ou le sous-traitant désignent le délégué à la protection des données sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées de la législation et des pratiques en matière de protection des données, et de sa capacité à accomplir les tâches énumérées à l’article 37. Le niveau de connaissances spécialisées requis est déterminé notamment en fonction du traitement des données effectué et de la protection exigée pour les données à caractère personnel traitées par le responsable du traitement ou le sous-traitant.

6. Le responsable du traitement ou le sous-traitant veillent à ce que d'éventuelles autres fonctions professionnelles du délégué à la protection des données soient compatibles avec les tâches et fonctions de cette personne en qualité de délégué à la protection des données et n'entraînent pas de conflit d'intérêts.

7. Le responsable du traitement ou le sous-traitant désignent un délégué à la protection des données pour une durée minimale de deux ans. Le mandat du délégué à la protection des données est reconductible. Durant son mandat, le délégué à la protection des données ne peut être démis de ses fonctions que s'il ne remplit plus les conditions requises pour l'exercice de celles-ci.

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

9. Le responsable du traitement ou le sous-traitant communiquent le nom et les coordonnées du délégué à la protection des données à l'autorité de contrôle et au public.

10. Les personnes concernées ont le droit de prendre contact avec le délégué à la protection des données au sujet de toutes questions relatives au traitement de données les concernant et de demander à exercer les droits que leur confère le présent règlement.

11. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables aux activités de base du responsable du traitement ou du sous-traitant, visées au paragraphe 1, point c), ainsi que les critères applicables aux qualités professionnelles du délégué à la protection des données visées au paragraphe 5.

Article 36
Fonction du délégué à la protection des données

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

2. Le responsable du traitement ou le sous-traitant veillent à ce que le délégué à la protection des données accomplisse ses missions et obligations en toute indépendance et ne reçoive aucune instruction en ce qui concerne l'exercice de sa fonction. Le délégué à la protection des données fait directement rapport à la direction du responsable du traitement ou du sous-traitant.

3. Le responsable du traitement ou le sous-traitant aident le délégué à la protection des données à exercer ses missions et fournissent le personnel, les locaux, les équipements et toutes autres ressources nécessaires à l'exécution des missions et obligations énoncées à l'article 37.

Article 37
Missions du délégué à la protection des données

1. Le responsable du traitement ou le sous-traitant confient au délégué à la protection des données au moins les missions suivantes:

   a) informer et conseiller le responsable du traitement ou le sous-traitant sur les obligations qui leur incombent en vertu du présent règlement et conserver une trace documentaire de cette activité et des réponses reçues;

   b) contrôler la mise en œuvre et l'application des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère

personnel, y compris la répartition des responsabilités, la formation du personnel participant aux traitements, et les audits s'y rapportant;

c) contrôler la mise en œuvre et l'application du présent règlement, notamment en ce qui concerne les exigences relatives à la protection des données dès la conception, à la protection des données par défaut et à la sécurité des données, ainsi que l'information des personnes concernées et l'examen des demandes présentées dans l'exercice de leurs droits au titre du présent règlement;

d) veiller à ce que la documentation visée à l'article 28 soit tenue à jour;

e) contrôler la documentation, la notification et la communication, prévues aux articles 31 et 32, et relatives aux violations de données à caractère personnel ;

f) vérifier que le responsable du traitement ou le sous-traitant a réalisé l'analyse d'impact relative à la protection des données, et que les demandes d'autorisation ou de consultation préalables ont été introduites, si elles sont requises au titre des articles 33 et 34;

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

h) faire office de point de contact pour l'autorité de contrôle sur les questions liées au traitement, et consulter celle-ci, le cas échéant, de sa propre initiative.

2. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables aux missions, à la certification, au statut, aux prérogatives et aux ressources du délégué à la protection des données au sens du paragraphe 1.

SECTION 5
CODES DE CONDUITE ET CERTIFICATION

Article 38
Codes de conduite

1. Les États membres, les autorités de contrôle et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des différents secteurs de traitement de données, à la bonne application des dispositions du présent règlement, en ce qui concerne notamment:

a) le traitement loyal et transparent des données;

b) la collecte des données;

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

d) les demandes formulées par les personnes concernées dans l'exercice de leurs droits;

e) l'information et la protection des enfants;

f) le transfert de données vers des pays tiers ou à des organisations internationales;

g) les mécanismes de suivi et visant à assurer le respect des dispositions du code par les responsables du traitement qui y adhèrent;

h) les procédures extrajudiciaires et les autres procédures de règlement des conflits permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées relatifs au traitement de données à caractère personnel, sans préjudice des droits des personnes concernées au titre des articles 73 et 75.

2. Les associations et les autres organisations représentant des catégories de responsables du traitement ou de sous-traitants dans un État membre qui ont l'intention d'élaborer des codes de conduite ou de modifier des codes de conduite existants ou d'en proroger la validité peuvent les soumettre à l'examen de l'autorité de contrôle de l'État membre concerné. L'autorité de contrôle peut rendre un avis sur la conformité, avec le présent règlement, du projet de code de conduite ou de la modification. Elle recueille les observations des personnes concernées ou de leurs représentants sur ces projets.

3. Les associations et les autres organisations représentant des catégories de responsables du traitement dans plusieurs États membres peuvent soumettre à la Commission des projets de codes de conduite ainsi que des modifications ou prorogations de codes de conduite existants.

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

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

Article 39
Certification

1. Les États membres et la Commission encouragent, en particulier au niveau européen, la mise en place de mécanismes de certification en matière de protection des données ainsi que de marques et de labels en matière de protection des données, qui permettent aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les responsables du traitement et les sous-traitants. Les mécanismes de certification en matière de protection des données contribuent à la bonne application du présent règlement, compte tenu des spécificités des divers secteurs et des différents traitements.

2. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables aux mécanismes de certification en matière de protection des données visés au paragraphe 1, y compris les conditions d'octroi et de révocation, et les exigences en matière de reconnaissance au sein de l'Union et dans les pays tiers.

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

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

Article 40
Principe général des transferts

Un transfert de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions énoncées 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 vers un autre pays tiers ou à une autre organisation internationale.

Article 41
Transferts assortis d'une décision relative au caractère adéquat du niveau de protection

1. Un transfert peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un secteur de traitement de données dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autre autorisation.

2. Lorsqu'elle apprécie le caractère adéquat du niveau de protection, la Commission prend en considération les éléments suivants:

   a) la primauté du droit, la législation pertinente en vigueur, tant générale que sectorielle, notamment en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal, les règles professionnelles et les mesures de sécurité qui sont respectées dans le pays en question ou par l'organisation internationale en question, ainsi que l'existence de droits effectifs et opposables, y compris un droit de recours administratif et judiciaire effectif des personnes concernées, notamment celles ayant leur résidence sur le territoire de l'Union et 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 l'organisation internationale en question, chargées d’assurer le respect des règles en matière de protection des données, d’assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle de l'Union et des États membres, et

c) les engagements internationaux souscrits par le pays tiers ou l'organisation internationale en question.

3. La Commission peut constater par voie de décision qu’un pays tiers, ou un territoire ou un secteur de traitement de données dans le pays tiers en question, ou une organisation internationale, assure un niveau de protection adéquat au sens du paragraphe 2. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

4. L'acte d'exécution précise son champ d'application géographique et sectoriel et, le cas échéant, cite le nom de l'autorité de contrôle mentionnée au paragraphe 2, point b).

5. La Commission peut constater par voie de décision qu'un pays tiers, ou un territoire ou un secteur de traitement de données dans ce pays tiers, ou une organisation internationale n'assure pas un niveau de protection adéquat au sens du paragraphe 2, notamment dans les cas où la législation pertinente, tant générale que sectorielle, en vigueur dans le pays tiers ou l'organisation internationale en question, ne garantit pas des droits effectifs et opposables, y compris un droit de recours administratif et judiciaire effectif des personnes concernées, notamment celles ayant leur résidence sur le territoire de l'Union et dont les données à caractère personnel sont transférées. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2, ou, en cas d’extrême urgence pour des personnes physiques en ce qui concerne leur droit à la protection de leurs données à caractère personnel, conformément à la procédure prévue à l'article 87, paragraphe 3.

6. Lorsque la Commission adopte une décision en vertu du paragraphe 5, tout transfert de données à caractère personnel vers le pays tiers, ou un territoire ou un secteur de traitement de données dans ce pays tiers, ou à l'organisation internationale en question est interdit, sans préjudice des articles 42 à 44. La Commission engage, au moment opportun, des consultations avec le pays tiers ou l'organisation internationale en vue de remédier à la situation résultant de la décision adoptée en vertu du paragraphe 5.

7. La Commission publie au *Journal officiel de l'Union européenne* une liste des pays tiers, des territoires et secteurs de traitement de données dans un pays tiers et des organisations internationales pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat était ou n'était pas assuré.

8. Les décisions adoptées par la Commission en vertu de l'article 25, paragraphe 6, ou de l'article 26, paragraphe 4, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation par la Commission.

Article 42

Transferts moyennant des garanties appropriées

1. Lorsque la Commission n'a pas adopté de décision en vertu l'article 41, le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale n'est possible que si le responsable du traitement ou le sous-traitant a offert des garanties appropriées en ce qui concerne la protection des données à caractère personnel dans un instrument juridiquement contraignant.

2. Les garanties appropriées visées au paragraphe 1 sont notamment fournies par:

   a) des règles d'entreprise contraignantes conformes à l'article 43; ou

   b) des clauses types de protection des données adoptées par la Commission. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2; ou

   c) des clauses types de protection des données adoptées par une autorité de contrôle conformément au mécanisme de contrôle de la cohérence prévu à l'article 57, lorsque la Commission a constaté leur applicabilité générale conformément à l'article 62, paragraphe 1, point b); ou

   d) des clauses contractuelles liant le responsable du traitement ou le sous-traitant et le destinataire des données, approuvées par une autorité de contrôle conformément au paragraphe 4.

3. Un transfert effectué en vertu de clauses types de protection des données ou de règles d'entreprise contraignantes telles que celles visés au paragraphe 2, points a), b) ou c), ne nécessite pas d'autre autorisation.

4. Lorsqu'un transfert est effectué en vertu de clauses contractuelles telles que celles visées au paragraphe 2, point d), le responsable du traitement ou le sous-traitant doit avoir obtenu l'autorisation préalable des clauses contractuelles par l'autorité de contrôle conformément à l'article 34, paragraphe 1, point a). Si le transfert est lié à un traitement qui porte sur des personnes concernées dans un ou plusieurs autres États membres, ou affecte sensiblement la libre circulation des données à caractère personnel dans l'Union, l'autorité de contrôle applique le mécanisme de contrôle de la cohérence prévu à l'article 57.

5. Lorsque les garanties appropriées quant à la protection de données à caractère personnel ne sont pas prévues dans un instrument juridiquement contraignant, le responsable du traitement ou le sous-traitant doit obtenir l'autorisation préalable du transfert ou d'un ensemble de transferts, ou de dispositions à insérer dans un régime administratif constituant le fondement du transfert. Une autorisation de cette nature accordée par l'autorité de contrôle doit être conforme à l'article 34, paragraphe 1, point a). Si le transfert est lié à un traitement qui porte sur des personnes concernées dans un ou plusieurs autres États membres, ou affecte sensiblement la libre circulation des données à caractère personnel dans l'Union, l'autorité de contrôle applique le mécanisme de contrôle de la cohérence prévu à l'article 57. Les autorisations accordées par une autorité de contrôle en vertu de l'article 26,

paragraphe 2, de la directive 95/46/CE demeurent valables jusqu'à leur modification, leur remplacement ou leur abrogation par la même autorité de contrôle.

Article 43
Transferts encadrés par des règles d'entreprise contraignantes

1. Une autorité de contrôle approuve des règles d'entreprise contraignantes conformément au mécanisme de contrôle de la cohérence prévu à l'article 58, à condition:

   a) qu'elles soient juridiquement contraignantes, qu'elles s'appliquent à toutes les entités du groupe d'entreprises du responsable du traitement ou du sous-traitant, y compris à leurs salariés, et que lesdites entités en assurent le respect;

   b) qu'elles confèrent expressément aux personnes concernées des droits opposables;

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

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

   a) la structure et les coordonnées du groupe d'entreprises et des entités qui le composent;

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

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

   d) les principes généraux de protection des données, notamment la limitation de la finalité, la qualité des données, la base juridique du traitement, le traitement de données à caractère personnel sensibles, 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 mesures en question;

   e) les droits des personnes concernées et les moyens de les exercer, notamment le droit de ne pas être soumis à une mesure fondée sur le profilage conformément à l'article 20, le droit de déposer une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres conformément à l'article 75 et d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes;

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

g) la manière dont les informations sur les règles d'entreprise contraignantes, notamment en ce qui concerne les éléments mentionnés aux points d), e) et f), sont fournies aux personnes concernées, conformément à l'article 11;

h) les missions du délégué à la protection des données, désigné conformément à l'article 35, notamment la surveillance, au sein du groupe d'entreprises, du respect des règles d'entreprise contraignantes, ainsi que le suivi de la formation et du traitement des réclamations;

i) les mécanismes mis en place au sein du groupe d'entreprises pour garantir que le respect des règles d'entreprise contraignantes est contrôlé;

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

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

3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables aux règles d'entreprise contraignantes au sens du présent article, notamment en ce qui concerne les critères applicables à leur approbation, l'application du paragraphe 2, points b), d), e) et f), aux règles d'entreprise contraignantes auxquelles adhèrent les sous-traitants, et les exigences nécessaires supplémentaires pour assurer la protection des données à caractère personnel des personnes concernées en question.

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

Article 44
Dérogations

1. En l'absence d'une décision relative au caractère adéquat du niveau de protection conformément à l'article 41 ou de garanties appropriées conformément à l'article 42, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peuvent être effectués qu'à condition que:

a) la personne concernée ait consenti au transfert envisagé, après avoir été informée des risques du transfert en raison de l'absence d'une décision relative au caractère adéquat du niveau de protection et de garanties appropriées; ou

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

c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu, dans l'intérêt de la personne concernée, entre le responsable du traitement et une autre personne physique ou morale; ou

d) le transfert soit nécessaire pour des motifs importants d'intérêt général; ou

e) le transfert soit nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice; ou

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

g) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions du droit de l'Union ou des États membres, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions prévues dans le droit de l'Union ou des États membres pour la consultation sont remplies dans le cas particulier; ou

h) le transfert soit nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou le sous-traitant, qu'il ne puisse pas être qualifié de fréquent ou de massif et que le responsable du traitement ou le sous-traitant ait évalué toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données et offert, sur la base de cette évaluation, des garanties appropriées au regard de la protection des données à caractère personnel, s'il y a lieu.

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

3. Lorsque le traitement s'effectue en vertu du paragraphe 1, point h), le responsable du traitement ou le sous-traitant prend particulièrement en considération la nature des données, la finalité et la durée du ou des traitements envisagés, ainsi que la situation dans le pays d'origine, le pays tiers et le pays de destination finale, et offre des garanties appropriées au regard de la protection des données à caractère personnel, s'il y a lieu.

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

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

6. Le responsable du traitement ou le sous-traitant atteste la matérialité, dans la documentation visée à l'article 28, de l'évaluation et des garanties appropriées offertes visées au paragraphe 1, point h), et informe l'autorité de contrôle du transfert.

7. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les «motifs importants d'intérêt général» au sens du paragraphe 1, point d), ainsi que les critères et exigences applicables aux garanties appropriées prévues au paragraphe 1, point h).

Article 45

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

1. La Commission et les autorités de contrôle prennent, à l'égard des pays tiers et des organisations internationales, les mesures appropriées pour:

   a) élaborer des mécanismes de coopération internationaux efficaces destinés à faciliter l'application de la législation relative à la protection des données à caractère personnel;

   b) se prêter mutuellement assistance sur le plan international dans la mise en application de la législation relative à la protection des données à caractère personnel, notamment par la notification, la transmission des réclamations, l'entraide pour les enquêtes et l'échange d'information, sous réserve de garanties appropriées pour la protection des données à caractère personnel et d'autres libertés et droits fondamentaux;

   c) associer les parties prenantes intéressées aux discussions et activités visant à développer la coopération internationale dans l'application de la législation relative à la protection des données à caractère personnel;

   d) favoriser l'échange et la conservation de la législation et des pratiques en matière de protection des données à caractère personnel.

2. Aux fins de l'application du paragraphe 1, la Commission prend les mesures appropriées pour intensifier les relations avec les pays tiers ou les organisations internationales, et en particulier leurs autorités de contrôle, lorsque la Commission a constaté par voie de décision qu'ils assuraient un niveau de protection adéquat au sens de l'article 41, paragraphe 3.

CHAPITRE VI
AUTORITÉS DE CONTRÔLE INDÉPENDANTES

SECTION 1
STATUT D'INDÉPENDANCE

Article 46

Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application du présent règlement et de contribuer à son application cohérente dans l'ensemble de l'Union, afin de protéger les libertés et droits

fondamentaux des personnes physiques en ce qui concerne le traitement de leurs données à caractère personnel et de faciliter la libre circulation de ces données au sein de l'Union. À cette fin, les autorités de contrôle coopèrent entre elles et avec la Commission.

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

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

Article 47
Indépendance

1. L'autorité de contrôle exerce en toute indépendance les missions et les pouvoirs qui lui sont confiés.

2. Dans l'accomplissement de leur mission, les membres de l'autorité de contrôle ne sollicitent ni n'acceptent d'instructions de quiconque.

3. Les membres de l'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. Après la cessation de leurs fonctions, les membres de l'autorité de contrôle sont tenus de respecter les devoirs d'honnêteté et de délicatesse quant à l'acceptation de certaines fonctions ou de certains avantages.

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

6. Chaque État membre veille à ce que l'autorité de contrôle dispose de son propre personnel, qui est désigné par le directeur de l'autorité de contrôle et est placé sous les ordres de celui-ci.

7. Les États membres veillent à ce que l'autorité de contrôle soit soumise à un contrôle financier qui ne menace pas son indépendance. Les États membres veillent à ce que l'autorité de contrôle dispose de budgets annuels propres. Les budgets sont rendus publics.

Article 48

Conditions générales applicables aux membres de l'autorité de contrôle

1. Chaque État membre prévoit que les membres de l’autorité de contrôle doivent être nommés soit par son parlement, soit par son gouvernement.

2. Les membres sont choisis parmi les personnes offrant toutes garanties d'indépendance et qui possèdent une expérience et une compétence notoires pour l'accomplissement de leurs fonctions, notamment dans le domaine de la protection des données à caractère personnel.

3. Les fonctions des membres prennent fin à l'échéance de leur mandat, en cas de démission ou de mise à la retraite d'office conformément au paragraphe 5.

4. Un membre peut être déclaré démissionnaire ou déchu du droit à pension ou d'autres avantages en tenant lieu par la juridiction nationale compétente, s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions ou s'il a commis une faute grave.

5. Un membre dont le mandat expire ou qui démissionne continue d'exercer ses fonctions jusqu'à la nomination d'un nouveau membre.

Article 49

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

Chaque État membre prévoit par voie législative, dans les limites du présent règlement:

a) l'établissement et le statut d’indépendance de l’autorité de contrôle;

b) les qualifications, l'expérience et les compétences requises pour exercer les fonctions de membre de l'autorité de contrôle;

c) les règles et les procédures pour la nomination des membres de l'autorité de contrôle, ainsi que les règles relatives aux activités ou emplois incompatibles avec leurs fonctions;

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

e) le caractère renouvelable ou non renouvelable du mandat des membres de l'autorité de contrôle;

f) le statut et les conditions communes régissant les fonctions des membres et agents de l’autorité de contrôle;

g) les règles et les procédures relatives à la cessation des fonctions des membres de l’autorité de contrôle, y compris lorsqu’ils ne remplissent plus les conditions nécessaires à l'exercice de leurs fonctions ou s'ils ont commis une faute grave.

Article 50
Secret professionnel

Les membres et agents de l'autorité de contrôle sont soumis, y compris après la cessation de leurs activités, à l'obligation de secret professionnel à l'égard de toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs fonctions officielles.

SECTION 2
FONCTIONS ET POUVOIRS

Article 51
Compétence

1. Chaque autorité de contrôle exerce, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au présent règlement.

2. Lorsque le traitement des données à caractère personnel a lieu dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant établis dans l'Union, et lorsque le responsable du traitement ou le sous-traitant sont établis dans plusieurs États membres, l'autorité de contrôle de l'État membre où se situe l'établissement principal du responsable du traitement ou du sous-traitant est compétente pour contrôler les activités de traitement du responsable du traitement ou du sous-traitant dans tous les États membres, sans préjudice des dispositions du chapitre VII du présent règlement.

3. L'autorité de contrôle n'est pas compétente pour contrôler les traitements effectués par les juridictions dans l'exercice de leur fonction juridictionnelle.

Article 52
Fonctions

1. L'autorité de contrôle:

   a) contrôle et assure l'application du présent règlement;

   b) reçoit les réclamations introduites par toute personne concernée ou par une association la représentant conformément à l'article 73, examine l'affaire pour autant que de besoin et informe la personne concernée ou l'association de l'état d'avancement de l'affaire et de l'issue de la réclamation dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire;

   c) partage des informations avec d'autres autorités de contrôle, leur fournit une assistance mutuelle et veille à la cohérence de l'application du présent règlement et des mesures prises pour en assurer le respect;

   d) effectue des enquêtes, soit de sa propre initiative, soit à la suite d'une réclamation ou à la demande d'une autre autorité de contrôle, et informe la

personne concernée, si elle l'a saisie d'une réclamation, du résultat de ses enquêtes dans un délai raisonnable;

e) surveille les faits nouveaux présentant un intérêt, dans la mesure où ils ont une incidence sur la protection des données à caractère personnel, notamment l'évolution des technologies de l'information et des communications et celle des pratiques commerciales;

f) est consultée par les institutions et organes de l'État membre sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel;

g) autorise les traitements prévus à l'article 34 et est consultée à leur sujet;

h) émet un avis sur les projets de codes de conduite prévus à l'article 38, paragraphe 2;

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

j) participe aux activités du comité européen de la protection des données.

2. Chaque autorité de contrôle sensibilise le public aux risques, aux règles, aux garanties et aux droits relatifs au traitement des données à caractère personnel. Les activités destinées spécifiquement aux enfants font l'objet d'une attention particulière.

3. L'autorité de contrôle, sur demande, conseille toute personne concernée dans l'exercice des droits découlant du présent règlement et, si nécessaire, coopère à cette fin avec les autorités de contrôle d'autres États membres.

4. Pour les réclamations visées au paragraphe 1, point b), l'autorité de contrôle fournit un formulaire de réclamation qui peut être rempli par voie électronique, sans exclure d'autres moyens de communication.

5. L'accomplissement des fonctions de l'autorité de contrôle est gratuit pour la personne concernée.

6. Lorsque les demandes sont manifestement excessives, en raison, notamment, de leur caractère répétitif, l'autorité de contrôle peut exiger le paiement de frais ou ne pas prendre les mesures sollicitées par la personne concernée. Il incombe à l'autorité de contrôle d'établir le caractère manifestement excessif de la demande.

Article 53
Pouvoirs

1. Chaque autorité de contrôle a le pouvoir:

a) d'informer le responsable du traitement ou le sous-traitant d'une violation alléguée des dispositions régissant le traitement des données à caractère personnel et, le cas échéant, d'ordonner au responsable du traitement ou au sous-traitant de remédier à cette violation par des mesures déterminées, afin d'améliorer la protection de la personne concernée;

b) d'ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes d'exercice des droits prévus par le présent règlement présentées par la personne concernée;

c) d'ordonner au responsable du traitement et au sous-traitant, et, le cas échéant, au représentant, de lui communiquer toute information utile pour l'exercice de ses fonctions;

d) de veiller au respect des autorisations et consultations préalables prévues à l'article 34;

e) d'adresser un avertissement ou une admonestation au responsable du traitement ou au sous-traitant;

f) d'ordonner la rectification, l'effacement ou la destruction de toutes les données lorsqu'elles ont été traitées en violation des dispositions du présent règlement et la notification de ces mesures aux tiers auxquels les données ont été divulguées;

g) d'interdire temporairement ou définitivement un traitement;

h) de suspendre les flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale;

i) d'émettre des avis sur toute question relative à la protection des données à caractère personnel;

j) d'informer le parlement national, le gouvernement ou d'autres institutions politiques, ainsi que le public, de toute question relative à la protection des données à caractère personnel.

2. Chaque autorité de contrôle dispose du pouvoir d'investigation lui permettant d'obtenir du responsable du traitement ou du sous-traitant:

a) l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'exercice de ses fonctions;

b) l'accès à tous les locaux, et notamment à toute installation ou à tout moyen de traitement, s'il existe un motif raisonnable de supposer qu'il s'y exerce une activité contraire au présent règlement.

Les pouvoirs visés au point b) sont exercés conformément au droit de l'Union et au droit des États membres.

3. Chaque autorité de contrôle a le pouvoir de porter toute violation du présent règlement à la connaissance de l'autorité judiciaire et d'ester en justice, notamment conformément à l'article 74, paragraphe 4, et à l'article 75, paragraphe 2.

4. Chaque autorité de contrôle a le pouvoir de sanctionner les infractions administratives, notamment celles énoncées à l'article 79, paragraphes 4, 5 et 6.

Article 54
Rapport d'activité

Chaque autorité de contrôle doit établir un rapport annuel sur son activité. Le rapport est présenté au parlement national; il est rendu public et mis à la disposition de la Commission et du comité européen de la protection des données.

CHAPITRE VII
COOPÉRATION ET COHÉRENCE

SECTION 1
COOPÉRATION

Article 55
Assistance mutuelle

1. Les autorités de contrôle se communiquent toute information utile et se prêtent une assistance mutuelle en vue de mettre en œuvre et d'appliquer le présent règlement de manière cohérente, et mettent en place des mesures pour coopérer efficacement entre elles. L'assistance mutuelle couvre notamment des demandes d'information et des mesures de contrôle, telles que les demandes d'autorisation et de consultation préalables, les inspections et la communication rapide d'informations sur l'ouverture de dossiers et sur leur évolution lorsque des personnes concernées dans plusieurs autres États membres sont susceptibles de faire l'objet de traitements.

2. Chaque autorité de contrôle prend toutes les mesures appropriées requises pour répondre à la demande d'une autre autorité de contrôle, sans délai et au plus tard un mois après la réception de la demande. Il peut s'agir, notamment, de la transmission d'informations utiles sur le déroulement d'une enquête ou de mesures répressives visant à faire cesser ou à interdire les traitements contraires au présent règlement.

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

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

   a) qu'elle ne soit pas compétente pour la traiter; ou

   b) qu'il soit incompatible avec les dispositions du présent règlement de donner suite à la demande.

5. L'autorité de contrôle requise informe l'autorité de contrôle requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour donner suite à la demande de l'autorité de contrôle requérante.

6. Les autorités de contrôle communiquent, par des moyens électroniques et dans les plus brefs délais, au moyen d'un formulaire type, les informations demandées par d'autres autorités de contrôle.

7. Une mesure prise à la suite d'une demande d'assistance mutuelle ne donne pas lieu à la perception de frais.

8. Lorsqu'une autorité de contrôle ne donne pas suite, dans un délai d'un mois, à la demande d'une autre autorité de contrôle, l'autorité de contrôle requérante a compétence pour adopter une mesure provisoire sur le territoire de l'État membre dont elle relève conformément à l'article 51, paragraphe 1, et saisit le comité européen de la protection des données de l'affaire conformément à la procédure prévue à l'article 57.

9. L'autorité de contrôle précise la durée de validité de la mesure provisoire ainsi adoptée. Cette durée ne peut excéder trois mois. L'autorité de contrôle communique sans délai ces mesures, dûment motivées, au comité européen de la protection des données et à la Commission.

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

Article 56
Opérations conjointes des autorités de contrôle

1. Afin d'intensifier la coopération et l'assistance mutuelle, les autorités de contrôle mettent en œuvre des missions d'enquête conjointes, des mesures répressives conjointes et d'autres opérations conjointes auxquelles participent des membres ou des agents des autorités de contrôle d'autres États membres, désignés par celles-ci.

2. Dans les cas où des personnes concernées dans plusieurs autres États membres sont susceptibles de faire l'objet de traitements, une autorité de contrôle de chacun des États membres en cause a le droit de participer aux missions d'enquête conjointes ou aux opérations conjointes, selon le cas. L'autorité de contrôle compétente invite l'autorité de contrôle de chacun de ces États membres à prendre part aux missions d'enquête conjointes ou aux opérations conjointes en cause et donne suite sans délai à toute demande d'une autorité de contrôle souhaitant participer aux opérations.

3. En tant qu'autorité de contrôle de l'État membre d'accueil, chaque autorité de contrôle peut, conformément à son droit national et avec l'accord de l'autorité de contrôle de l'État membre d'origine, confier des compétences de puissance publique, notamment des missions d'enquête, aux membres ou aux agents de l'autorité de contrôle de l'État membre d'origine participant à des opérations conjointes ou admettre, pour autant que le droit dont relève l'autorité de contrôle de l'État membre d'accueil le permette, que les membres ou les agents de l'autorité de contrôle de l'État membre d'origine exercent leurs compétences de puissance publique conformément au droit dont relève

l'autorité de contrôle de l'État membre d'origine. Ces compétences de puissance publique ne peuvent être exercées que sous l'autorité et, en règle générale, en présence de membres ou d'agents de l'autorité de contrôle de l'État membre d'accueil. Les membres ou agents de l'autorité de contrôle de l'État membre d'origine sont soumis au droit national de l'autorité de contrôle de l'État membre d'accueil. L'autorité de contrôle de l'État membre d'accueil assume la responsabilité de leurs actes.

4. Les autorités de contrôle définissent les modalités pratiques des actions de coopération particulières.

5. Lorsqu'une autorité de contrôle ne se conforme pas, dans un délai d'un mois, à l'obligation énoncée au paragraphe 2, les autres autorités de contrôle ont compétence pour prendre une mesure provisoire sur le territoire de leur État membre, conformément à l'article 51, paragraphe 1.

6. L'autorité de contrôle précise la durée de validité de toute mesure provisoire prévue au paragraphe 5. Cette durée ne peut excéder trois mois. L'autorité de contrôle communique sans délai ces mesures, dûment motivées, au comité européen de la protection des données et à la Commission, et fait examiner l'affaire dans le cadre du mécanisme prévu à l'article 57.

SECTION 2
COHÉRENCE

Article 57
Mécanisme de contrôle de la cohérence

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

Article 58
Avis du comité européen de la protection des données

1. Avant d'adopter une mesure visée au paragraphe 2, toute autorité de contrôle communique le projet de mesure au comité européen de la protection des données et à la Commission.

2. L'obligation énoncée au paragraphe 1 s'applique à toute mesure destinée à produire des effets juridiques et qui:

   a) se rapporte aux traitements liés à l'offre de biens ou de services à des personnes concernées dans plusieurs États membres ou à l'observation de leur comportement; ou

   b) est susceptible d'affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union; ou

c) vise à l'adoption d'une liste des traitements devant faire l'objet d'une consultation préalable conformément à l'article 34, paragraphe 5, ou

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

e) vise à l'autorisation de clauses contractuelles telles que celles visées à l'article 42, paragraphe 2, point d), ou

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

3. Toute autorité de contrôle ou le comité européen de la protection des données peut demander que toute question soit traitée dans le cadre du mécanisme de contrôle de la cohérence, notamment lorsqu'une autorité de contrôle omet de soumettre pour examen un projet de mesure visé au paragraphe 2 ou ne respecte pas les obligations relatives à l'assistance mutuelle découlant de l'article 55 ou aux opérations conjointes découlant de l'article 56.

4. En vue d'assurer l'application correcte et cohérente du présent règlement, la Commission peut demander que toute question soit examinée dans le cadre du mécanisme de contrôle de la cohérence.

5. Les autorités de contrôle et la Commission communiquent par voie électronique, au moyen d'un formulaire type, toutes les informations utiles, notamment, selon le cas, un résumé des faits, le projet de mesure et les motifs rendant nécessaire l'adoption de la mesure.

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

7. Si ses membres en décident ainsi à la majorité simple, ou à la demande de toute autorité de contrôle ou de la Commission, le comité européen de la protection des données émet un avis sur l'affaire dans un délai d'une semaine après la communication des informations utiles conformément au paragraphe 5. L'avis est adopté dans un délai d'un mois à la majorité simple des membres du comité européen de la protection des données. Le président du comité européen de la protection des données informe sans retard indu l'autorité de contrôle visée, selon le cas, au paragraphe 1 ou au paragraphe 3, la Commission et l'autorité de contrôle compétente en vertu de l'article 51 de l'avis et le publie.

8. L'autorité de contrôle visée au paragraphe 1 et l'autorité de contrôle compétente en vertu de l'article 51 tiennent compte de l'avis du comité européen de la protection des données et communiquent par voie électronique au président du conseil européen de la protection des données et à la Commission, dans un délai de deux semaines après avoir été informée de l'avis par ledit président, si elles maintiennent ou modifient le projet de mesure, et, le cas échéant, communiquent le projet de mesure modifié, au moyen d'un formulaire type.

Article 59
Avis de la Commission

1. Dans un délai de dix semaines à compter de la date à laquelle une question a été soulevée conformément à l'article 58, ou au plus tard dans un délai de six semaines dans le cas visé à l'article 61, la Commission peut, afin d'assurer l'application correcte et cohérente du présent règlement, adopter un avis sur les questions soulevées conformément aux articles 58 ou 61.

2. Lorsque la Commission a adopté un avis en vertu du paragraphe 1, l'autorité de contrôle concernée tient le plus grand compte de l'avis de la Commission et indique à la Commission et au comité européen de la protection des données si elle entend maintenir ou modifier son projet de mesure.

3. Pendant le délai visé au paragraphe 1, l'autorité de contrôle s'abstient d'adopter le projet de mesure.

4. Lorsque l'autorité de contrôle concernée n'entend pas se conformer à l'avis de la Commission, elle en informe la Commission et le comité européen de la protection des données dans le délai visé au paragraphe 1 et motive sa décision. Dans cette éventualité, l'autorité de contrôle s'abstient d'adopter le projet de mesure pendant un délai supplémentaire d'un mois.

Article 60
Suspension d'un projet de mesure

1. Dans un délai d'un mois à compter de la communication prévue à l'article 59, paragraphe 4, et lorsque la Commission nourrit des doutes sérieux quant à savoir si le projet de mesure permet de garantir la bonne application du présent règlement ou s'il est susceptible, au contraire, d'aboutir à une application non cohérente de celui-ci, la Commission, en tenant compte de l'avis formulé par le comité européen de la protection des données conformément à l'article 58, paragraphe 7, ou à l'article 61, paragraphe 2, peut adopter une décision motivée enjoignant à l'autorité de contrôle de suspendre l'adoption du projet de mesure lorsqu'une telle suspension apparaît requise pour:

   a) rapprocher les positions divergentes de l'autorité de contrôle et du comité européen de la protection des données, si un tel rapprochement apparaît encore possible; ou

   b) adopter une mesure en vertu de l'article 62, paragraphe 1, point a).

2. La Commission précise la durée de la suspension, qui ne peut excéder douze mois.

3. Pendant le délai visé au paragraphe 2, l'autorité de contrôle ne peut pas adopter le projet de mesure.

Article 61
Procédure d'urgence

1. Dans des circonstances exceptionnelles, lorsqu'une autorité de contrôle considère qu'il est urgent d'intervenir pour protéger les intérêts de personnes concernées, notamment lorsque le risque existe que l'exercice effectif du droit d'une personne concernée soit considérablement entravé par une modification de la situation existante, pour éviter des inconvénients majeurs ou pour d'autres raisons, elle peut, par dérogation à la procédure prévue à l'article 58, adopter sans délai des mesures provisoires ayant une durée de validité déterminée. L'autorité de contrôle communique sans délai ces mesures, dûment motivées, au comité européen de la protection des données et à la Commission.

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

3. Toute autorité de contrôle peut, en motivant sa demande, et notamment l'urgence d'intervenir, demander un avis d'urgence lorsque l'autorité de contrôle compétente n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les intérêts de personnes concernées.

4. Par dérogation à l'article 58, paragraphe 7, un avis d'urgence tel que celui visé aux paragraphes 2 et 3 est adopté dans un délai de deux semaines à la majorité simple des membres du comité européen de la protection des données.

Article 62
Actes d'exécution

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

   a) statuer sur l'application correcte du présent règlement conformément à ses objectifs et exigences quant aux questions soulevées par les autorités de contrôle conformément à l'article 58 ou à l'article 61, quant à une question au sujet de laquelle une décision motivée a été adoptée en vertu de l'article 60, paragraphe 1, ou quant à une affaire dans laquelle une autorité de contrôle omet de soumettre pour examen un projet de mesure et a indiqué qu'elle n'entendait pas se conformer à l'avis de la Commission adopté en vertu de l'article 59;

   b) statuer, dans le délai fixé à l'article 59, paragraphe 1, sur l'applicabilité générale de projets de clauses types de protection des données telles que celles visées à l'article 58, paragraphe 2, point d);

   c) définir la forme et les procédures d'application du mécanisme de contrôle de la cohérence prévu par la présente section;

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

Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

2. Pour des raisons impérieuses d'urgence dûment justifiées, tenant aux intérêts de personnes concernées dans les cas visés au paragraphe 1, point a), la Commission adopte des actes d'exécution immédiatement applicables conformément à la procédure visée à l'article 87, paragraphe 3. Ces actes restent en vigueur pendant une période n'excédant pas douze mois.

3. L'absence ou l'adoption d'une mesure au titre de la présente section est sans préjudice de toute autre mesure adoptée par la Commission en vertu des traités.

Article 63
Mise à exécution

1. Aux fins de l'application du présent règlement, toute mesure exécutoire de l'autorité de contrôle d'un État membre est mise à exécution dans tous les États membres concernés.

2. Lorsqu'une autorité de contrôle omet de soumettre un projet de mesure pour examen dans le cadre du mécanisme de contrôle de la cohérence en violation de l'article 58, paragraphes 1 à 5, la mesure de l'autorité de contrôle est dénuée de validité juridique et de caractère exécutoire.

SECTION 3
COMITE EUROPEEN DE LA PROTECTION DES DONNEES

Article 64
Comité européen de la protection des données

1. Il est institué un comité européen de la protection des données.

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

3. Lorsque, dans un État membre, plusieurs autorités de contrôle sont chargées de surveiller l'application des dispositions du présent règlement, celles-ci désignent le directeur de l'une d'entre elles comme représentant commun.

4. La Commission a le droit de participer aux activités et réunions du comité européen de la protection des données et désigne un représentant. Le président du comité européen de la protection des données informe sans délai la Commission de toutes les activités du comité européen de la protection des données.

Article 65
Indépendance

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

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

Article 66
Missions du comité européen de la protection des données

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

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

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

   c) de faire le bilan de l'application pratique des lignes directrices, recommandations et bonnes pratiques visées au point b) et de faire régulièrement rapport à la Commission sur ces mesures;

   d) d'émettre des avis sur les projets de décision des autorités de contrôle conformément au mécanisme de contrôle de la cohérence prévu à l'article 57;

   e) de promouvoir la coopération et l'échange bilatéral et multilatéral effectif d'informations et de pratiques entre les autorités de contrôle;

   f) de promouvoir l'élaboration de programmes de formation conjoints et de faciliter les échanges de personnel entre autorités de contrôle, ainsi que, le cas échéant, avec les autorités de contrôle de pays tiers ou d'organisations internationales;

   g) de promouvoir l'échange, avec des autorités de contrôle de la protection des données de tous pays, de connaissances et de documentation sur la législation et les pratiques en matière de protection des données.

2. Lorsque la Commission consulte le comité européen de la protection des données, elle peut fixer un délai dans lequel il doit lui fournir les conseils demandés, selon l'urgence de la question.

3. Le comité européen de la protection des données transmet ses avis, lignes directrices, recommandations et bonnes pratiques à la Commission et au comité visé à l'article 87, et il les publie.

4. La Commission informe le comité européen de la protection des données de la suite qu'elle a réservée aux avis, lignes directrices, recommandations et bonnes pratiques publiées par ledit comité.

Article 67
Rapports

1. Le comité européen de la protection des données informe la Commission, régulièrement et en temps utile, des résultats de ses activités. Il établit un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans l'Union et dans les pays tiers.

   Le rapport doit notamment présenter le bilan de l'application pratique des lignes directrices, des recommandations et des bonnes pratiques visées à l'article 66, paragraphe 1, point c).

2. Le rapport est publié et communiqué au Parlement européen, au Conseil et à la Commission.

Article 68
Procédure

1. Le comité européen de la protection des données prend ses décisions à la majorité simple de ses membres.

2. Le comité européen de la protection des données établit son règlement intérieur et détermine ses modalités de fonctionnement. Il adopte notamment des dispositions relatives à la poursuite de l'exercice des fonctions lorsque le mandat d'un membre expire ou en cas de démission d'un membre, à la création de sous-groupes sur des sujets ou pour des secteurs spécifiques et aux procédures qu'il applique en ce qui concerne le mécanisme de contrôle de la cohérence visé à l'article 57.

Article 69
Présidence

1. Le comité européen de la protection des données élit son président et deux vice-présidents en son sein. L'un des vice-présidents est le contrôleur européen de la protection des données, à moins qu'il ait été élu président.

2. Le président et les vice-présidents sont élus pour un mandat de cinq ans renouvelable.

Article 70
Missions du président

1. Le président a pour mission:

   a) de convoquer les réunions du comité européen de la protection des données et d'établir son ordre du jour;

   b) de veiller à l'exécution, dans les délais, des missions du comité européen de la protection des données, notamment en ce qui concerne le mécanisme de contrôle de la cohérence prévu à l'article 57.

2. Le comité européen de la protection des données fixe dans son règlement intérieur la répartition des tâches entre le président et les vice-présidents.

Article 71
Secrétariat

1. Le comité européen de la protection des données dispose d'un secrétariat. Celui-ci est assuré par le contrôleur européen de la protection des données.

2. Le secrétariat fournit, sous la direction du président, un soutien analytique, administratif et logistique au comité européen de la protection des données.

3. Le secrétariat est notamment chargé:

   a) de la gestion courante du comité européen de la protection des données;

   b) de la communication entre les membres du comité européen de la protection des données, son président et la Commission, et de la communication avec d'autres institutions et le public;

   c) du recours à des moyens électroniques pour la communication interne et externe;

   d) de la traduction des informations utiles;

   e) de la préparation et du suivi des réunions du comité européen de la protection des données;

   f) de la préparation, de la rédaction et de la publication d'avis et d'autres textes adoptés par le comité européen de la protection des données.

Article 72
Confidentialité

1. Les débats du comité européen de la protection des données sont confidentiels.

2. Les documents présentés aux membres du comité européen de la protection des données, aux experts et aux représentants de tierces parties sont confidentiels, sauf si l'accès à ces documents est accordé conformément au règlement (CE) n° 1049/2001

ou si le comité européen de la protection des données les rend publics de toute autre manière.

3. Les membres du comité européen de la protection des données, ainsi que les experts et les représentants de tierces parties, sont tenus de respecter les obligations de confidentialité établies au présent article. Le président veille à ce que les experts et les représentants de tierces parties aient connaissance des exigences qu'ils sont tenus de respecter en matière de confidentialité.

CHAPITRE VIII
RECOURS, RESPONSABILITÉ ET SANCTIONS

Article 73
Droit d'introduire une réclamation auprès d'une autorité de contrôle

1. Sans préjudice de tout autre recours administratif ou judiciaire, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle dans tout État membre si elle considère que le traitement de données à caractère personnel la concernant n'est pas conforme au présent règlement.

2. Tout organisme, organisation ou association qui œuvre à la protection des droits et des intérêts des personnes concernées à l'égard de la protection de leurs données à caractère personnel et qui a été valablement constitué conformément au droit d'un État membre a le droit d'introduire une réclamation auprès d'une autorité de contrôle dans tout État membre au nom d'une ou de plusieurs personnes concernées s'il considère que les droits dont jouit une personne concernée en vertu du présent règlement ont été violés à la suite du traitement de données à caractère personnel.

3. Indépendamment d'une réclamation introduite par une personne concernée, tout organisme, organisation ou association visé au paragraphe 2 a le droit de saisir une autorité de contrôle dans tout État membre d'une réclamation s'il considère qu'il y a eu violation de données à caractère personnel.

Article 74
Droit à un recours juridictionnel contre une autorité de contrôle

1. Toute personne physique ou morale a le droit de former un recours juridictionnel contre les décisions d'une autorité de contrôle qui la concernent.

2. Toute personne concernée a le droit de former un recours juridictionnel en vue d'obliger l'autorité de contrôle à donner suite à une réclamation, en l'absence d'une décision nécessaire pour protéger ses droits ou lorsque l'autorité de contrôle, n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de sa réclamation conformément à l'article 52, paragraphe 1, point b).

3. Les actions contre une autorité de contrôle sont intentées devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie.

4. Toute personne concernée affectée par une décision d'une autorité de contrôle d'un État membre autre que celui dans lequel elle a sa résidence habituelle peut demander à l'autorité de contrôle de l'État membre dans lequel elle a sa résidence habituelle d'intenter une action en son nom contre l'autorité de contrôle compétente de l'autre État membre.

5. Les États membres mettent à exécution les décisions définitives des juridictions visées au présent article.

Article 75

Droit à un recours juridictionnel contre un responsable du traitement ou un sous-traitant

1. Sans préjudice de tout recours administratif qui lui est ouvert, notamment le droit prévu à l'article 73 de saisir une autorité de contrôle d'une réclamation, toute personne physique dispose d'un recours juridictionnel si elle considère qu'il a été porté atteinte aux droits que lui confère le présent règlement, à la suite du traitement de données à caractère personnel la concernant, effectué en violation du présent règlement.

2. Une action contre un responsable du traitement ou un sous-traitant est intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement. Une telle action peut aussi être intentée devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle, sauf si le responsable du traitement est une autorité publique agissant dans l'exercice de ses prérogatives de puissance publique.

3. Lorsqu'une procédure qui concerne la même mesure, décision ou pratique est en cours dans le cadre du mécanisme de contrôle de la cohérence prévu à l'article 58, une juridiction peut surseoir à statuer dans le litige dont elle est saisie, sauf si l'urgence de l'affaire pour la protection des droits de la personne concernée ne permet pas d'attendre l'issue de la procédure en cours dans le cadre du mécanisme de contrôle de la cohérence.

4. Les États membres mettent à exécution les décisions définitives des juridictions visées au présent article.

Article 76

Règles communes pour les procédures juridictionnelles

1. Tout organisme, organisation ou association visé à l'article 73, paragraphe 2, est habilité à exercer les droits prévus aux articles 74 et 75 au nom d'une ou de plusieurs personnes concernées.

2. Chaque autorité de contrôle a le droit d'ester en justice et de saisir une juridiction en vue de faire respecter les dispositions du présent règlement ou d'assurer la cohérence de la protection des données à caractère personnel au sein de l'Union.

3. Lorsqu'une juridiction compétente d'un État membre a des motifs raisonnables de croire qu'une procédure parallèle est en cours dans un autre État membre, elle prend

contact avec la juridiction compétente de cet autre État membre pour obtenir confirmation de l'existence de cette procédure parallèle.

4. Lorsqu'une procédure parallèle dans un autre État membre porte sur la même mesure, décision ou pratique, la juridiction peut surseoir à statuer.

5. Les États membres veillent à ce que les voies de recours disponibles dans le droit national permettent l'adoption rapide de mesures, y compris par voie de référé, visant à mettre un terme à toute violation alléguée et à prévenir toute nouvelle atteinte aux intérêts concernés.

Article 77
Droit à réparation et responsabilité

1. Toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec le présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

2. Lorsque plusieurs responsables du traitement ou sous-traitants ont participé au traitement, chacun d'entre eux est solidairement responsable de la totalité du montant du dommage.

3. Le responsable du traitement ou le sous-traitant peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Article 78
Sanctions pénales

1. Les États membres prévoient les sanctions pénales applicables aux violations des dispositions du présent règlement et prennent toutes les mesures nécessaires pour garantir leur application, y compris lorsque le responsable du traitement n'a pas respecté l'obligation de désigner un représentant. Les sanctions pénales ainsi prévues doivent être effectives, proportionnées et dissuasives.

2. Lorsque le responsable du traitement a désigné un représentant, les sanctions sont appliquées au représentant, sans préjudice de toute procédure de sanction susceptible d'être engagée contre le responsable du traitement.

3. Chaque État membre notifie à la Commission les dispositions de la législation qu'il adopte en vertu du paragraphe 1, au plus tard à la date figurant à l'article 91, paragraphe 2, et, sans délai, toute modification ultérieure les affectant.

Article 79
Sanctions administratives

1. Chaque autorité de contrôle est habilitée à infliger des sanctions administratives en conformité avec le présent article.

2. Dans chaque cas, la sanction administrative doit être effective, proportionnée et dissuasive. Le montant de l'amende administrative est fixé en tenant dûment compte de la nature, de la gravité et de la durée de la violation, du fait que l'infraction a été commise de propos délibéré ou par négligence, du degré de responsabilité de la personne physique ou morale en cause et de violations antérieurement commises par elle, des mesures et procédures techniques et d'organisation mises en œuvre conformément à l'article 23 et du degré de coopération avec l'autorité de contrôle en vue de remédier à la violation.

3. Lors du premier manquement non intentionnel au présent règlement, l'autorité de contrôle peut donner un avertissement par écrit mais n'impose aucune sanction:

   a) lorsqu'une personne physique traite des données à caractère personnel en l'absence de tout intérêt commercial; ou

   b) lorsqu'une entreprise ou un organisme comptant moins de 250 salariés traite des données à caractère personnel uniquement dans le cadre d'une activité qui est accessoire à son activité principale.

4. L'autorité de contrôle inflige une amende pouvant s'élever à 250 000 EUR ou, dans le cas d'une entreprise, à 0,5 % de son chiffre d'affaires annuel mondial, à quiconque, de propos délibéré ou par négligence:

   a) ne prévoit pas les mécanismes permettant aux personnes concernées de formuler des demandes ou ne répond pas sans tarder ou sous la forme requise aux personnes concernées conformément à l'article 12, paragraphes 1 et 2;

   b) perçoit des frais pour les informations ou pour les réponses aux demandes de personnes concernées en violation de l'article 12, paragraphe 4.

5. L'autorité de contrôle inflige une amende pouvant s'élever à 500 000 EUR ou, dans le cas d'une entreprise, à 1 % de son chiffre d'affaires annuel mondial, à quiconque, de propos délibéré ou par négligence:

   a) ne fournit pas les informations, fournit des informations incomplètes ou ne fournit pas les informations de façon suffisamment transparente à la personne concernée conformément à l'article 11, à l'article 12, paragraphe 3, et à l'article 14;

   b) ne fournit pas un accès à la personne concernée, ne rectifie pas les données à caractère personnel conformément aux articles 15 et 16 ou ne communique pas les informations en cause à un destinataire conformément à l'article 13;

   c) ne respecte pas le droit à l'oubli numérique ou à l'effacement, omet de mettre en place des mécanismes garantissant le respect des délais ou ne prend pas toutes les mesures nécessaires pour informer les tiers qu'une personne concernée demande l'effacement de tout lien vers les données à caractère personnel, ou la copie ou la reproduction de ces données conformément à l'article 17.

   d) omet de fournir une copie des données à caractère personnel sous forme électronique ou fait obstacle à ce que la personne concernée transmette ses

données à caractère personnel à une autre application en violation de l'article 18;

e) omet de définir ou ne définit pas suffisamment les obligations respectives des responsables conjoints du traitement conformément à l'article 24;

f) ne tient pas, ou pas suffisamment, à jour la documentation conformément à l'article 28, à l'article 31, paragraphe 4, et à l'article 44, paragraphe 3;

g) ne respecte pas, lorsque des catégories particulières de données ne sont pas concernées, conformément aux articles 80, 82 et 83, les règles en matière de liberté d'expression, les règles sur le traitement de données à caractère personnel en matière d'emploi ou les conditions de traitement à des fins de recherche historique, statistique et scientifique.

6. L'autorité de contrôle inflige une amende pouvant s'élever à 1 000 000 EUR ou, dans le cas d'une entreprise, à 2 % de son chiffre d'affaires annuel mondial, à quiconque, de propos délibéré ou par négligence:

a) traite des données à caractère personnel sans base juridique ou sans base juridique suffisante à cette fin ou ne respecte pas les conditions relatives au consentement conformément aux articles 6, 7 et 8;

b) traite des catégories particulières de données en violation des articles 9 et 81;

c) ne respecte pas une opposition ou ne se conforme pas à l'obligation prévue à l'article 19;

d) ne respecte pas les conditions relatives aux mesures fondées sur le profilage conformément à l'article 20;

e) omet d'adopter des règles internes ou de mettre en œuvre les mesures requises pour assurer et prouver le respect des obligations énoncées aux articles 22, 23 et 30;

f) omet de désigner un représentant conformément à l'article 25;

g) traite des données à caractère personnel ou donne l'instruction d'en effectuer le traitement en violation des obligations, énoncées aux articles 26 et 27, en matière de traitement réalisé pour le compte d'un responsable du traitement;

h) omet de signaler ou de notifier une violation de données à caractère personnel, ou omet de notifier la violation en temps utile ou de façon complète à l'autorité de contrôle ou à la personne concernée conformément aux articles 31 et 32;

i) omet d'effectuer une analyse d'impact relative à la protection des données ou traite des données à caractère personnel sans autorisation préalable ou consultation préalable de l'autorité de contrôle conformément aux articles 33 et 34;

j) omet de désigner un délégué à la protection des données ou de veiller à ce que les conditions pour l'accomplissement de ses missions soient réunies conformément aux articles 35, 36 et 37;

k) fait un usage abusif d'une marque ou d'un label de protection des données au sens de l'article 39;

l) effectue ou donne l'instruction d'effectuer, vers un pays tiers ou à une organisation internationale, un transfert de données qui n'est pas autorisé par une décision relative au caractère adéquat du niveau de protection, couvert par des garanties appropriées ou par une dérogation conformément aux articles 40 à 44;

m) ne respecte pas une injonction, une interdiction temporaire ou définitive de traitement ou la suspension de flux de données par l'autorité de contrôle conformément à l'article 53, paragraphe 1;

n) ne respecte pas l'obligation de prêter assistance, de répondre ou de fournir des informations utiles à l'autorité de contrôle ou de lui donner accès aux locaux conformément à l'article 28, paragraphe 3, à l'article 29, à l'article 34, paragraphe 6, et à l'article 53, paragraphe 2;

o) ne respecte pas les règles de protection du secret professionnel conformément à l'article 84.

7. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86 aux fins d'adapter le montant des amendes administratives prévues aux paragraphes 4, 5 et 6, en tenant compte des critères énoncés au paragraphe 2.

CHAPITRE IX
DISPOSITIONS RELATIVES À DES SITUATIONS PARTICULIÈRES DE TRAITEMENT DES DONNÉES

Article 80
Traitements de données à caractère personnel et liberté d'expression

1. Les États membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations aux dispositions sur les principes généraux du chapitre II, sur les droits de la personne concernée du chapitre III, sur le responsable du traitement et le sous-traitant du chapitre IV, sur le transfert de données à caractère personnel vers des pays tiers et à des organisations internationales du chapitre V, sur les autorités de contrôle indépendantes du chapitre VI et sur la coopération et la cohérence du chapitre VII, pour concilier le droit à la protection des données à caractère personnel avec les règles régissant la liberté d'expression.

2. Chaque État membre notifie à la Commission les dispositions de la législation qu'il adopte en vertu du paragraphe 1, au plus tard à la date figurant à l'article 91, paragraphe 2, et, sans délai, toute modification ultérieure les affectant.

Article 81

Traitements de données à caractère personnel relatives à la santé

1. Dans les limites du présent règlement et conformément à l'article 9, paragraphe 2, point h), les traitements de données à caractère personnel relatives à la santé doivent être effectués sur la base du droit de l'Union ou de la législation d'un État membre qui prévoit des garanties appropriées et spécifiques des intérêts légitimes de la personne concernée, et doivent être nécessaires:

   a) aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et lorsque le traitement de ces données est effectué par un praticien de la santé soumis au secret professionnel, ou par une autre personne également soumise à une obligation de confidentialité équivalente, par le droit d'un État membre ou par des réglementations arrêtées par les autorités nationales compétentes; ou

   b) pour des motifs d'intérêt général dans le domaine de la santé publique, tels que la protection contre les menaces transfrontières graves pour la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité, entre autres pour les médicaments ou les équipements médicaux; ou

   c) pour d'autres motifs d'intérêt général dans des domaines tels que la protection sociale, particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance-maladie.

2. Les traitements de données à caractère personnel relatives à la santé qui sont nécessaires à des fins de recherche historique, statistique ou scientifique, tels que les registres de patients établis pour améliorer les diagnostics, distinguer entre des types de maladies similaires et préparer des études en vue de thérapies sont soumis aux conditions et aux garanties énoncées à l'article 83.

3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage d'autres motifs d'intérêt général dans le domaine de la santé publique au sens du paragraphe 1, point b), ainsi que les critères et exigences applicables aux garanties encadrant le traitement de données à caractère personnel aux fins prévues au paragraphe 1.

Article 82

Traitements de données en matière d'emploi

1. Dans les limites du présent règlement, les États membres peuvent adopter, par voie législative, un régime spécifique pour le traitement des données à caractère personnel des salariés en matière d'emploi, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de la santé et de la sécurité au travail, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.

2. Chaque État membre notifie à la Commission les dispositions de la législation qu'il adopte en vertu du paragraphe 1, au plus tard à la date figurant à l'article 91, paragraphe 2, et, sans délai, toute modification ultérieure les affectant.

3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et les exigences applicables aux garanties encadrant le traitement de données à caractère personnel aux fins prévues au paragraphe 1.

Article 83

Traitements de données à des fins de recherche historique, statistique et scientifique

1. Dans les limites du présent règlement, les données à caractère personnel ne peuvent faire l'objet d'un traitement à des fins de recherche historique, statistique ou scientifique que si:

   a) ces finalités ne peuvent être atteintes d'une autre façon par le traitement de données qui ne permettent pas ou ne permettent plus d'identifier la personne concernée;

   b) les données permettant de rattacher des informations à une personne concernée identifiée ou identifiable sont conservées séparément des autres informations, à condition que ces fins puissent être atteintes de cette manière.

2. Les organismes effectuant des recherches historiques, statistiques ou scientifiques ne peuvent publier ou divulguer des données à caractère personnel que si:

   a) la personne concernée a donné son consentement, sous réserve du respect des conditions énoncées à l'article 7;

   b) la publication de données à caractère personnel est nécessaire pour présenter les résultats de la recherche ou pour faciliter la recherche, sous réserve que les intérêts ou les libertés ou les droits fondamentaux de la personne concernée ne prévalent pas sur l'intérêt de la recherche; ou

   c) la personne concernée a rendu publiques les données en cause.

3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et les exigences applicables au traitement de données à caractère personnel visé aux paragraphes 1 et 2, ainsi que toute limitation nécessaire des droits d'information et d'accès de la personne concernée, et de préciser les conditions et garanties applicables aux droits de la personne concernée dans les circonstances en cause.

Article 84

Obligations de secret

1. Dans les limites du présent règlement, les États membres peuvent adopter des règles spéciales afin de définir les pouvoirs d'investigation des autorités de contrôle visés à l'article 53, paragraphe 2, en ce qui concerne les responsables du traitement ou les

sous-traitants qui sont soumis, en vertu du droit national ou de réglementations arrêtées par les autorités nationales compétentes, à une obligation de secret professionnel ou d'autres obligations de secret équivalentes, lorsque de telles règles sont nécessaires et proportionnées pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret. Ces règles ne sont applicables qu'en ce qui concerne les données à caractère personnel que le responsable du traitement ou le sous-traitant a reçues ou s'est procurées dans le cadre d'une activité couverte par ladite obligation de secret.

2. Chaque État membre notifie à la Commission les dispositions qu'il adopte conformément au paragraphe 1, au plus tard à la date visée à l'article 91, paragraphe 2, et, sans délai, toute modification ultérieure les affectant.

Article 85
Règles existantes des églises et associations religieuses en matière de protection des données

1. Lorsque, dans un État membre, des églises et des associations ou communautés religieuses appliquent, à la date d'entrée en vigueur du présent règlement, un ensemble complet de règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, elles peuvent continuer d'appliquer lesdites règles à condition de les mettre en conformité avec les dispositions du présent règlement.

2. Les églises et les associations religieuses qui appliquent un ensemble complet de règles conformément au paragraphe 1 prévoient la création d'une autorité de contrôle indépendante conformément au chapitre VI du présent règlement.

CHAPITRE X
ACTES DÉLÉGUÉS ET ACTES D'EXÉCUTION

Article 86
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. La délégation de pouvoir visée à l'article 6, paragraphe 5, à l'article 8, paragraphe 3, à l'article 9, paragraphe 3, à l'article 12, paragraphe 5, à l'article 14, paragraphe 7, à l'article 15, paragraphe 3, à l'article 17, paragraphe 9, à l'article 20, paragraphe 6, à l'article 22, paragraphe 4, à l'article 23, paragraphe 3, à l'article 26, paragraphe 5, à l'article 28, paragraphe 5, à l'article 30, paragraphe 3, à l'article 31, paragraphe 5, à l'article 32, paragraphe 5, à l'article 33, paragraphe 6, à l'article 34, paragraphe 8, à l'article 35, paragraphe 11, à l'article 37, paragraphe 2, à l'article 39, paragraphe 2, à l'article 43, paragraphe 3, à l'article 44, paragraphe 7, à l'article 79, paragraphe 6, à l'article 81, paragraphe 3, à l'article 82, paragraphe 3, et à l'article 83, paragraphe 3, est conférée à la Commission pour une durée indéterminée à compter de la date d'entrée en vigueur du présent règlement.

3. La délégation de pouvoir visée à l'article 6, paragraphe 5, à l'article 8, paragraphe 3, à l'article 9, paragraphe 3, à l'article 12, paragraphe 5, à l'article 14, paragraphe 7, à l'article 15, paragraphe 3, à l'article 17, paragraphe 9, à l'article 20, paragraphe 6, à l'article 22, paragraphe 4, à l'article 23, paragraphe 3, à l'article 26, paragraphe 5, à l'article 28, paragraphe 5, à l'article 30, paragraphe 3, à l'article 31, paragraphe 5, à l'article 32, paragraphe 5, à l'article 33, paragraphe 6, à l'article 34, paragraphe 8, à l'article 35, paragraphe 11, à l'article 37, paragraphe 2, à l'article 39, paragraphe 2, à l'article 43, paragraphe 3, à l'article 44, paragraphe 7, à l'article 79, paragraphe 6, à l'article 81, paragraphe 3, à l'article 82, paragraphe 3, et à l'article 83, paragraphe 3, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui y est précisée. Elle n'affecte pas la validité des actes délégués déjà en vigueur.

4. Dès qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.

5. Un acte délégué adopté en vertu de l'article 6, paragraphe 5, de l'article 8, paragraphe 3, de l'article 9, paragraphe 3, de l'article 12, paragraphe 5, de l'article 14, paragraphe 7, de l'article 15, paragraphe 3, de l'article 17, paragraphe 9, de l'article 20, paragraphe 6, de l'article 22, paragraphe 4, de l'article 23, paragraphe 3, de l'article 26, paragraphe 5, de l'article 28, paragraphe 5, de l'article 30, paragraphe 3, de l'article 31, paragraphe 5, de l'article 32, paragraphe 5, de l'article 33, paragraphe 6, de l'article 34, paragraphe 8, de l'article 35, paragraphe 11, de l'article 37, paragraphe 2, de l'article 39, paragraphe 2, de l'article 43, paragraphe 3, de l'article 44, paragraphe 7, de l'article 79, paragraphe 6, de l'article 81, paragraphe 3, de l'article 82, paragraphe 3, et de l'article 83, paragraphe 3, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 87
Procédure de comité

1. La Commission est assistée par un comité. Ce comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 8 du règlement (UE) n° 182/2011 s'applique, en liaison avec son article 5.

CHAPITRE XI
DISPOSITIONS FINALES

Article 88
Abrogation de la directive 95/46/CE

1. La directive 95/46/CE est abrogée.

2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE s'entendent comme faites au comité européen de la protection des données institué par le présent règlement.

Article 89
Relation avec la directive 2002/58/CE et modification de cette directive

1. Le présent règlement n'impose pas d'obligations supplémentaires aux personnes physiques ou morales quant au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union en ce qui concerne les domaines dans lesquels elles sont soumises à des obligations spécifiques ayant le même objet que celles énoncées dans la directive 2002/58/CE.

2 L'article 1er, paragraphe 2, de la directive 2002/58/CE est supprimé.

Article 90
Évaluation

La Commission présente périodiquement des rapports sur l'évaluation et la révision du présent règlement au Parlement européen et au Conseil. Le premier rapport est présenté au plus tard quatre ans après l'entrée en vigueur du présent règlement. Les rapports suivants sont ensuite présentés tous les quatre ans. Pour autant que de besoin, la Commission soumet les propositions voulues pour modifier le présent règlement et pour adapter d'autres instruments juridiques, en tenant compte, notamment, de l'évolution de la technologie de l'information et des progrès de la société de l'information. Les rapports sont publiés.

Article 91

Entrée en vigueur et application

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

2. Il est applicable à compter du [*deux ans à compter de la date visée au paragraphe 1*].

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

Fait à Bruxelles, le

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

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

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

1.3. Nature de la proposition/de l'initiative

1.4. Objectif(s)

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

1.6. Durée et incidence financière

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système de gestion et de contrôle

2.3. Mesures de prévention des fraudes et irrégularités

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

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

3.2. Incidence estimée sur les dépenses

3.2.1. Synthèse de l'incidence estimée sur les dépenses

3.2.2. Incidence estimée sur les crédits opérationnels

3.2.3. Incidence estimée sur les crédits de nature administrative

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

La présente fiche financière présente plus en détail les exigences en termes de dépenses administratives afin de mettre en pratique la réforme de la protection des données, comme l'explique l'analyse d'impact correspondante. La réforme contient deux propositions législatives: un règlement général sur la protection des données et une directive 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 des sanctions pénales. La présente fiche financière couvre l'incidence budgétaire des deux instruments.

Selon la répartition des tâches, des ressources sont demandées par la Commission et par le contrôleur européen de la protection des données (CEPD).

En ce qui concerne la Commission, les ressources nécessaires sont déjà incluses dans les perspectives financières proposées pour la période 2014-2020. La protection des données est l'un des objectifs du programme «Droits et citoyenneté», qui soutiendra également des mesures visant à mettre en pratique le cadre juridique. Les crédits administratifs, qui couvrent les besoins en personnel, sont compris dans le budget administratif de la DG JUST.

Pour ce qui est du CEPD, les ressources nécessaires devront être prises en compte dans les budgets annuels respectifs le concernant. Elles sont détaillées à l'annexe de la présente fiche financière. Afin de fournir les ressources nécessaires aux nouvelles missions du comité européen de la protection des données, dont le CEPD assurera le secrétariat, il y aura lieu de procéder à une reprogrammation de la rubrique 5 des perspectives financières 2014-2020.

1.1. Dénomination de la proposition/de l'initiative

Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données). Proposition de directive du Parlement européen et du Conseil 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.

1.2. Domaine(s) politique(s) concerné(s) dans la structure ABM/ABB[49]

Justice - Protection des données à caractère personnel

[49] ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

L'incidence budgétaire concerne la Commission et le CEPD. L'incidence sur le budget de la Commission est détaillée dans les tableaux de la présente fiche financière. Les dépenses opérationnelles relèvent du programme «Droits et citoyenneté» et ont déjà été prises en compte dans la fiche financière dudit programme, car les dépenses administratives font partie de l'enveloppe prévue pour la DG Justice. Les éléments concernant le CEPD figurent en annexe.

1.3. Nature de la proposition/de l'initiative

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

☐ La proposition/l'initiative porte **sur une action nouvelle suite à un projet pilote/une action préparatoire**[50]

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

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

1.4. Objectif(s)

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

La réforme a pour but de parachever la réalisation des objectifs initiaux, en tenant compte des évolutions et des défis nouveaux, à savoir:

- accroître l'efficacité du droit fondamental à la protection des données et permettre aux personnes physiques de contrôler les données qui les concernent, notamment dans le contexte des évolutions technologiques et d'une mondialisation accrue;

- développer la dimension «marché intérieur» de la protection des données en réduisant la fragmentation, en renforçant la cohérence et en simplifiant l'environnement réglementaire, afin de supprimer les coûts inutiles et de réduire la charge administrative.

En outre, l'entrée en vigueur du traité de Lisbonne, notamment l'introduction d'une nouvelle base juridique (article 16 du TFUE), donne la possibilité d'atteindre un nouvel objectif, à savoir

- mettre en place un cadre global pour la protection des données, couvrant tous les domaines.

[50] Tel(le) que visé(e) à l'article 49, paragraphe 6, point a) ou b), du règlement financier.

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

Objectif spécifique n° 1

Garantir une application cohérente des règles relatives à la protection des données

Objectif spécifique n° 2

Rationaliser le système actuel de gouvernance afin de contribuer à assurer une mise en œuvre plus cohérente

Activité(s) ABM/ABB concernée(s)

[…]

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

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

En ce qui concerne les responsables du traitement de données, les entités tant publiques que privées bénéficieront d'une sécurité juridique accrue résultant d'une harmonisation et d'une clarification des règles et procédures de l'UE en matière de protection des données, permettant d'instaurer des conditions homogènes et d'assurer une application cohérente de ces règles de protection des données, ainsi que de réduire considérablement la charge administrative.

Les personnes physiques auront une meilleure maîtrise des données qui les concernent et auront confiance dans l'environnement numérique, tout en restant protégées même lorsque ces données sont traitées à l'étranger. Elles constateront en outre que la responsabilité des personnes ou entités chargées du traitement des données à caractère personnel est renforcée.

Un régime global de protection des données couvrira également les domaines de la police et de la justice, reprenant et élargissant l'ancien troisième pilier.

1.4.4. Indicateurs de résultats et d'incidences

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

(voir l'analyse d'impact, section 8)
Les indicateurs feront l'objet d'une évaluation périodique et couvriront les éléments suivants:

- le temps et les moyens financiers consacrés par les responsables du traitement de données à la mise en œuvre de la législation «dans d'autres États membres»,
- les ressources allouées aux autorités de contrôle,
- les délégués à la protection des données désignés dans les organisations publiques et privées,
- l'utilisation des analyses d'impact relatives à la protection des données,
- le nombre de réclamations introduites par des personnes concernées et la réparation qu'elles ont obtenue,
- le nombre d'affaires ayant entraîné des poursuites à l'encontre de responsables du traitement des données,
- les amendes infligées aux responsables du traitement de données au titre des violations de la protection des données qui leur sont imputables.

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

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

Les divergences actuelles dans la transposition, l'interprétation et l'application de la directive par les États membres ***entravent le fonctionnement du marché intérieur et la coopération entre les autorités publiques concernant les politiques de l'UE.*** Cette situation est contraire à l'objectif fondamental de la directive, qui est de faciliter la libre circulation des données à

caractère personnel dans le marché intérieur. Le développement rapide des nouvelles technologies et de la mondialisation aggrave encore ce problème.

Les personnes physiques ne jouissent pas des mêmes droits en matière de protection des données, en raison d'une fragmentation, d'une mise en œuvre et d'une application manquant de cohérence dans les divers États membres. En outre, ***les personnes physiques n'ont généralement pas connaissance de l'utilisation qui est faite de leurs données à caractère personnel, ou n'en ont pas la maîtrise,*** et ne peuvent donc exercer leurs droits de manière effective.

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

Les États membres ne peuvent réduire à eux seuls les problèmes dans la situation actuelle. Il en est notamment ainsi pour les problèmes résultant de la fragmentation dans les législations nationales qui mettent en œuvre le cadre réglementaire de l'UE relatif à la protection des données. Il est donc pleinement justifié d'instaurer un cadre juridique pour la protection des données au niveau de l'UE. Il y a précisément lieu de définir un cadre harmonisé et cohérent permettant un transfert aisé des données à caractère personnel au-delà des frontières nationales au sein de l'UE, tout en assurant une protection effective à toutes les personnes physiques dans l'ensemble de l'UE.

1.5.3. Leçons tirées d'expériences similaires

Les propositions s'appuient sur l'expérience acquise avec la directive 95/46/CE et les problèmes rencontrés du fait de la transposition et de la mise en œuvre fragmentaires de cette directive, qui ont entravé la réalisation des deux objectifs visés, à savoir un niveau élevé de protection des données et un marché intérieur pour la protection des données.

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

Le présent train de mesures réformant la protection des données vise à instaurer un cadre solide, cohérent et moderne au niveau de l'UE dans ce domaine, qui soit neutre sur le plan technologique et résistant à l'épreuve du temps pour plusieurs décennies. Il profitera aux personnes physiques, en renforçant leurs droits en matière de protection des données, notamment dans l'environnement numérique, et simplifiera l'environnement juridique des entreprises et du secteur public, favorisant ainsi le développement de l'économie numérique dans l'ensemble du marché intérieur de l'UE et au-delà, conformément aux objectifs de la stratégie Europe 2020.

L'essentiel du train de mesures réformant la protection des données est composé:

– d'un règlement qui remplace la directive 95/46/CE;

– d'une directive 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.

Ces propositions législatives sont accompagnées d'un rapport sur la mise en œuvre, par les États membres, de ce qui constitue actuellement le principal instrument de protection des données dans l'UE dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale, à savoir la décision-cadre 2008/977/JAI.

1.6. Durée et incidence financière

☐ Proposition/initiative à **durée limitée**

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

2. ☐ Incidence financière de AAAA jusqu'en AAAA

☑ Proposition/initiative à **durée illimitée**

1. Mise en œuvre avec une période de démarrage de 2014 à 2016,

2. puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) de gestion prévu(s)[51]

☑ **Gestion centralisée directe** par la Commission

☐ **Gestion centralisée indirecte** par délégation de tâches d'exécution à:

3. ☐ des agences exécutives

4. ☐ des organismes créés par les Communautés[52]

5. ☐ des organismes publics nationaux/organismes avec mission de service public

3. ☐ des personnes chargées de l'exécution d'actions spécifiques en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné au sens de l'article 49 du règlement financier

☐ **Gestion partagée** avec les États membres

☐ **Gestion décentralisée** avec des pays tiers

☐ **Gestion conjointe** avec des organisations internationales (***à préciser***)

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

Remarques

//

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

[52] Tels que visés à l'article 185 du règlement financier.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

La première évaluation aura lieu quatre ans après l'entrée en vigueur des instruments juridiques. Une clause explicite de révision, sur la base de laquelle la Commission évaluera la mise en œuvre, est comprise dans ces instruments. La Commission communiquera ensuite son évaluation au Parlement européen et au Conseil. De nouvelles évaluations devront avoir lieu tous les quatre ans. La Commission appliquera ses méthodes d'évaluation. Ces évaluations seront effectuées à l'aide d'études ciblées relatives à la mise en œuvre des instruments juridiques, de questionnaires adressés aux autorités nationales de protection des données, de discussions d'experts, d'ateliers, d'enquêtes Eurobaromètre, etc.

2.2. Système de gestion et de contrôle

2.2.1. Risque(s) identifié(s)

Une analyse d'impact a été réalisée concernant la réforme du cadre de la protection des données dans l'UE, pour accompagner les propositions de règlement et de directive.

Les nouveaux instruments juridiques mettront en place un mécanisme de contrôle de la cohérence, afin que des autorités de contrôle indépendantes dans les États membres appliquent ce cadre de manière homogène et cohérente. Ce mécanisme sera utilisé par le comité européen de la protection des données, composé des directeurs des autorités de contrôle nationales et du contrôleur européen de la protection des données (CEPD), qui remplacera l'actuel groupe de travail «Article 29». Le CEPD assurera le secrétariat de cet organe.

En cas de décisions éventuellement divergentes prises par les autorités des États membres, le comité européen de la protection des données sera consulté, pour obtenir son avis sur la question. En cas d'échec de cette procédure, ou si une autorité de contrôle refuse de se conformer à l'avis dudit comité, la Commission pourrait, afin d'assurer l'application correcte et cohérente du présent règlement, émettre un avis ou, le cas échéant, adopter une décision lorsqu'elle nourrit des doutes sérieux quant à savoir si le projet de mesure permet de garantir la bonne application du présent règlement ou s'il est susceptible, au contraire, d'aboutir à une application non cohérente de celui-ci.

Le mécanisme de contrôle de la cohérence nécessite l'octroi de ressources supplémentaires au CEPD pour qu'il en assure le secrétariat (12 ETP ainsi que les crédits administratifs et opérationnels appropriés, notamment pour les systèmes et traitements informatiques), et à la Commission pour la gestion des cas soumis au mécanisme (5 ETP ainsi que les crédits administratifs et opérationnels correspondants).

2.2.2. Moyen(s) de contrôle prévu(s)

Des méthodes de contrôle existantes appliquées par le CEPD et la Commission couvriront les crédits supplémentaires.

2.3. Mesures de prévention des fraudes et irrégularités

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

Des méthodes de contrôle existantes appliquées par le CEPD et la Commission couvriront les crédits supplémentaires.

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

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

1. Lignes budgétaires existantes

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

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro [Intitulé…………...…….]	CD/CND[53]	de pays AELE[54]	de pays candidats[55]	de pays tiers	au sens de l'article 18, paragraphe 1, point a) bis, du règlement financier

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

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

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

3.2. Incidence estimée sur les dépenses

3.2.1. Synthèse de l'incidence estimée sur les dépenses

En millions d'EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel:	**Numéro**	

			Année **N**[56]**= 2014**	Année **N+1**	Année **N+2**	Année **N+3**	… insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			**TOTAL**
• Crédits opérationnels										
Numéro de la ligne budgétaire	Engagements	(1)								
	Paiements	(2)								
Numéro de la ligne budgétaire	Engagements	(1a)								
	Paiements	(2a)								
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[57]										
Numéro de la ligne budgétaire		(3)								
TOTAL des crédits pour la DG	Engagements	=1+1a +3								
	Paiements	=2+2a +3								

[56] L'année N est l'année au cours de laquelle la mise en œuvre de la proposition/de l'initiative commence.

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

• TOTAL des crédits opérationnels	Engagements	(4)								
	Paiements	(5)								
• TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		(6)								
TOTAL des crédits pour la RUBRIQUE 3 du cadre financier pluriannuel	Engagements	=4+ 6								
	Paiements	=5+ 6								

Si plusieurs rubriques sont concernées par la proposition / initiative:

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

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

En millions d'EUR (à la 3e décimale)

		Année **N= 2014**	Année **2015**	Année **2016**	Année **2017**	Année **2018**	Année **2019**	Année **2020**	**TOTAL**
DG: JUST									
• Ressources humaines		2,922	2,922	2,922	2,922	2,922	2,922	2,922	**20,454**

• Autres dépenses administratives		0,555	0,555	0,555	0,555	0,555	0,555	0,555	**3,885**
TOTAL DG JUST		**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

TOTAL des crédits pour la RUBRIQUE 5 du cadre financier pluriannuel	(Total engagements = Total paiements)	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

En millions d'EUR (à la 3e décimale)

		Année **N**[58]	Année **N+1**	Année **N+2**	Année **N+3**	… insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 5 du cadre financier pluriannuel	Engagements	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**
	Paiements	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

[58] L'année N est l'année au cours de laquelle la mise en œuvre de la proposition/de l'initiative commence.

3.2.2. Incidence estimée sur les crédits opérationnels

6. ☑ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

Un niveau élevé de protection des données à caractère personnel est également l'un des objectifs du programme «Droits et citoyenneté».

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

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

Indiquer les objectifs et les réalisations ⇩			Année **N=2014**		Année **N+1**		Année **N+2**		Année **N+3**		…insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)						**TOTAL**	
			REALISATIONS															
	Type de réalisation [59]	Coût moyen de la réalisation	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nbre total de réalisations	Coût total
OBJECTIF SPÉCIFIQUE n° 1																		
- Réalisation	Dossiers[60]																	
Sous-total objectif spécifique n° 1																		
OBJECTIF SPÉCIFIQUE n° 2																		
- Réalisation	Cas[61]																	

59 Les réalisations se réfèrent aux produits et services qui seront fournis (ex: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

60 Avis, décisions, réunions du comité relatives aux procédures.

61 Cas traités dans le cadre du mécanisme de contrôle de la cohérence.

Sous-total objectif spécifique n° 2																
COÛT TOTAL																

3.2.3. Incidence estimée sur les crédits de nature administrative

3.2.3.1. Synthèse

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

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

En millions d'EUR (à la 3e décimale)

	Année **N**[62] **2014**	Année **2015**	Année **2016**	Année **2017**	Année **2018**	Année **2019**	Année **2020**	**TOTAL**
RUBRIQUE 5 du cadre financier pluriannuel								
Ressources humaines	2,922	2,922	2,922	2,922	2,922	2,922	2,922	**20,454**
Autres dépenses administratives	0,555	0,555	0,555	0,555	0,555	0,555	0,555	**3,885**
Sous-total RUBRIQUE 5 du cadre financier pluriannuel	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**
Hors RUBRIQUE 5[63] **du cadre financier pluriannuel**								
Ressources humaines								
Autres dépenses de nature administrative								
Sous-total hors RUBRIQUE 5 du cadre financier pluriannuel								
TOTAL	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

62 L'année N est l'année au cours de laquelle la mise en œuvre de la proposition/de l'initiative commence.

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

3.2.3.2. Besoins estimés en ressources humaines

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

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

Estimation à exprimer en équivalent temps plein (ou au maximum avec une décimale)

		Année **2014**	Année **2015**	Année **2016**	Année **2017**	Année **2018**	Année **2019**	Année **2020**
• **Emplois du tableau des effectifs (fonctionnaires et agents temporaires)**								
XX 01 01 01 (au siège et dans les bureaux de représentation de la Commission)		22	22	22	22	22	22	22
XX 01 01 02 (en délégation)								
• **Personnel externe (en équivalent temps plein - ETP)**[64]								
XX 01 02 01 (AC, END, INT de l'«enveloppe globale»)		2	2	2	2	2	2	2
XX 01 02 02 (AC, AL, END, INT et JED dans les délégations)								
XX 01 04 ***yy*** [65]	- au siège[66]							
	- en délégation							
XX 01 05 02 (AC, END, INT sur recherche indirecte)								
10 01 05 02 (AC, END, INT sur recherche directe)								
Autres lignes budgétaires (préciser)								
TOTAL		**24**	**24**	**24**	**24**	**24**	**24**	**24**

XX est le domaine politique ou titre concerné.

Avec la réforme, la Commission sera chargée d'accomplir de nouvelles missions dans le domaine de la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel, outre celles qu'elle mène déjà bien. Ces missions supplémentaires se rapportent essentiellement à la mise en œuvre du nouveau mécanisme de contrôle de la cohérence, qui garantira une application homogène de la législation harmonisée en matière de protection des données, à l'évaluation du caractère adéquat du niveau de protection dans les pays tiers, dont la Commission aura la responsabilité exclusive, et à la préparation des mesures d'exécution et des actes délégués. La Commission continuera à mener à bien les

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

65 Sous-plafond de personnel externe sur crédits opérationnels (anciennes lignes «BA»).

66 Essentiellement pour les Fonds structurels, le Fonds européen agricole pour le développement rural (Feader) et le Fonds européen pour la pêche (FEP).

autres missions qui lui incombent actuellement (notamment l'élaboration de politiques, le suivi de la transposition, les activités de sensibilisation, les réclamations, etc.).

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

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Gestionnaires de dossiers, mettant en œuvre le mécanisme de contrôle de la cohérence pour la protection des données afin de garantir l'application uniforme des règles de l'UE en matière de protection des données. Ils sont chargés notamment d'effectuer des enquêtes et des recherches sur les cas soumis par les autorités des États membres en vue d'une décision, de négocier avec les États membres et de préparer les décisions de la Commission. Sur la base de l'expérience récente, entre 5 et 10 cas par an pourraient nécessiter un recours au mécanisme de contrôle de la cohérence. La gestion des demandes relatives au caractère adéquat du niveau de protection exige une interaction directe avec le pays demandeur, éventuellement la gestion d'études réalisées par des experts concernant les conditions appliquées dans le pays en question, l'évaluation de ces conditions, la préparation des décisions correspondantes de la Commission et de la procédure, y compris au sein du comité qui assiste la Commission et de tout organe spécialisé, le cas échéant. L'expérience acquise indique que l'on peut s'attendre à un maximum de quatre demandes par an relatives au caractère adéquat du niveau de protection. Le processus d'adoption de mesures d'exécution comprend des mesures préparatoires, telles que des documents thématiques, des recherches et des consultations publiques, ainsi que l'élaboration de l'instrument lui-même et la gestion du processus de négociation dans les comités et autres groupes concernés, ainsi que les contacts avec les parties intéressées de manière générale. Dans les domaines qui exigent des orientations plus précises, il est possible de traiter jusqu'à trois mesures d'exécution par an, alors que le processus peut durer jusqu'à 24 mois, selon l'intensité des consultations.
Personnel externe	Services administratifs et de secrétariat

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

12. ☐La proposition/l'initiative est compatible avec le *prochain* cadre financier pluriannuel.

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

Le tableau ci-dessous indique les montants de ressources financières nécessaires chaque année pour que le CEPD accomplisse ses nouvelles missions, consistant à assurer le secrétariat du comité européen de la protection des données, et les procédures et outils afférents pendant la

période des prochaines perspectives financières, outre les missions déjà incluses dans la planification.

Année	2014	2015	2016	2017	2018	2019	2020	Total
Personnel etc.	1,555	1,555	1,543	1,543	1,543	1,543	1,543	10,823
Opérations	0,850	1,500	1,900	1,900	1,500	1,200	1,400	10,250
Total	**2,405**	**3,055**	**3,443**	**3,443**	**3,043**	**2,743**	**2,943**	**21,073**

14. ☐La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel[67].

3.2.5. Participation de tiers au financement

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

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

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

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

3.3. Incidence estimée sur les recettes

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

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

- ☐ sur les ressources propres
- ☐ sur les recettes diverses

En millions d'euros (à la 3e décimale)

Ligne budgétaire de recette:	Montants inscrits pour l'exercice en	Incidence de la proposition/de l'initiative[68]				
		Année	Année	Année	Année	… insérer autant d'années que nécessaire,

[67] Voir points 19 et 24 de l'accord interinstitutionnel.

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

	cours	**N**	**N+1**	**N+2**	**N+3**	pour refléter la durée de l'incidence (cf. point 1.6)		

Pour les recettes diverses qui seront «affectées», préciser la(les) ligne(s) budgétaire(s) de dépense concernée(s).
Préciser la méthode de calcul de l'effet sur les recettes.

Annexe à la fiche financière législative concernant la proposition de règlement du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Méthode appliquée et principales hypothèses retenues

Les coûts liés aux nouvelles missions qui seront menées à bien par le contrôleur européen de la protection des données (CEPD), résultant des deux propositions, ont été estimés pour les dépenses de personnel sur la base des coûts exposés actuellement par la Commission dans le cadre de missions analogues.

Le CEPD hébergera le secrétariat du comité européen de la protection des données qui remplace le groupe de travail «Article 29». Compte tenu de la charge de travail actuelle de la Commission pour cette mission, cela signifie que 3 ETP supplémentaires sont nécessaires, ainsi que les dépenses administratives et opérationnelles correspondantes. Cette charge de travail deviendra effective avec l'entrée en vigueur du règlement.

En outre, le CEPD jouera un rôle dans le mécanisme de contrôle de la cohérence qui devrait nécessiter 5 ETP, ainsi que dans le développement et l'exploitation d'un outil informatique commun aux autorités nationales de protection des données, qui exigera 2 personnes supplémentaires.

Le calcul de l'augmentation du budget requis pour le personnel au cours des sept premières années est présenté plus en détail dans le tableau ci-dessous. Un second tableau indique le budget opérationnel requis. Ces éléments seront repris dans le budget de l'UE sous la section IX (contrôleur européen de la protection des données).

Type de coût	**Calcul**	**Montant (en milliers)**							
		2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**
Traitements et indemnités									
- de la présidence du CEPD		0,300	0,300	0,300	0,300	0,300	0,300	0,300	2,100
- dont ceux des fonctionnaires et agents temporaires	=7*0,127	0,889	0,889	0,889	0,889	0,889	0,889	0,889	6,223
- dont ceux des END	=1*0,073	0,073	0,073	0,073	0,073	0,073	0,073	0,073	0,511
- dont ceux des agents contractuels	=2*0,064	0,128	0,128	0,128	0,128	0,128	0,128	0,128	0,896
Dépenses de recrutement	=10*0,005	0,025	0,025	0,013	0,013	0,013	0,013	0,013	0,113
Frais de mission		0,090	0,090	0,090	0,090	0,090	0,090	0,090	0,630
Autres dépenses, formation	=10*0,005	0,050	0,050	0,050	0,050	0,050	0,050	0,050	0,350

Dépenses administratives totales		**1,555**	**1,555**	**1,543**	**1,543**	**1,543**	**1,543**	**1,543**	**10,823**

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Agents administratifs chargés du secrétariat du comité de la protection des données. Outre l'appui logistique, incluant les questions budgétaires et contractuelles, il s'agit de préparer des ordres du jour de réunions et des invitations d'experts, d'effectuer des recherches sur les thèmes figurant au programme du groupe, de gérer les documents relatifs aux travaux du groupe, en tenant compte des exigences en matière de protection des données, de confidentialité et d'accès du public. En intégrant tous les sous-groupes et groupes d'experts, jusqu'à 50 réunions et procédures de décision pourraient devoir être organisées chaque année. Gestionnaires de dossiers mettant en œuvre le mécanisme de contrôle de la cohérence pour la protection des données afin de garantir l'application uniforme des règles de l'UE en matière de protection des données. Ils sont chargés notamment d'effectuer des enquêtes et des recherches sur les cas soumis par les autorités des États membres en vue d'une décision, de négocier avec les États membres et de préparer les décisions de la Commission. Sur la base de l'expérience récente, entre 5 et 10 cas par an pourraient nécessiter un recours au mécanisme de contrôle de la cohérence. L'outil informatique simplifiera l'interaction opérationnelle entre les autorités nationales de protection des données et les responsables du traitement qui sont tenus de partager des informations avec les autorités publiques. Le(s) membre(s) du personnel responsable(s) assurera(assureront) le contrôle de qualité, la gestion de projets et le suivi budgétaire des processus informatiques concernant la spécification des exigences, la mise en œuvre et l'exploitation des systèmes.
Personnel externe	Services administratifs et de secrétariat

Dépenses pour le CEPD liées à des missions spécifiques

Indiquer les objectifs et les réalisations ⇩			Année **N=2014**		Année **N+1**		Année **N+2**		Année **N+3**		… insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)						**TOTAL**	
			REALISATIONS															
	Type de réalisation [69]	Coût moyen de la réalisation	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nombre de réalisations	Coût	Nbre total de réalisations	Coût total
OBJECTIF SPÉCIFIQUE n° 1 [70]			Secrétariat pour le comité de la protection des données															
- Réalisation	Cas [71]	0,010	30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
Sous-total objectif spécifique n° 1			30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
OBJECTIF SPÉCIFIQUE n° 2			Mécanisme de contrôle de la cohérence															
- Réalisation	Dossiers [72]	0,050	5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	59	2,950
Sous-total objectif spécifique n° 2			5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	59	2,950
OBJECTIF SPÉCIFIQUE n° 3			Outil informatique commun pour les autorités nationales de protection des données (CEPD)															
- Réalisation	Cas [73]	0,100	3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500	41	4,100
Sous-total objectif spécifique n° 3			3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500	41	4,100
COÛT TOTAL			38	0,850	56	1,500	69	1,900	69	1,900	64	1,500	61	1,200	63	1,400	420	10,250

69 Les réalisations se réfèrent aux produits et services qui seront fournis (ex: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

70 Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)...».

71 Cas traités dans le cadre du mécanisme de contrôle de la cohérence.

72 Avis, décisions, réunions du comité relatives aux procédures.

73 Les totaux par année donnent une estimation des efforts à fournir pour développer et exploiter les outils informatiques.