COMMISSION EUROPÉENNE

Bruxelles, le 25.1.2012
COM(2012) 10 final

2012/0010 (COD)

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

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

Le présent exposé des motifs précise l'approche suivie pour mettre en place le nouveau cadre juridique de la protection des données à caractère personnel dans l'Union européenne, telle que définie dans la communication COM(2012) 9 final. Ce 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.

Le présent exposé des motifs porte sur cette seconde proposition législative.

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[1], 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 divers instruments contenant des règles spécifiques de protection des données dans le domaine de la coopération policière et judiciaire en matière pénale[2] (ancien troisième pilier), notamment la décision-cadre 2008/977/JAI[3].

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[4]. Dans sa résolution sur le programme de Stockholm, le Parlement européen[5] 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[6], 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

---

1 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, (ci-après «la directive»).

2 Voir la liste complète à l'annexe 3 de l'analyse d'impact [SEC(2012) 72].

3 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»).

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

5 Voir la 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).

6 COM(2010) 171final.

politiques européennes. Le plan d'action soulignait que *«[d]ans une société mondialisée, caractérisée par une évolution technologique rapide et des échanges d'informations ne connaissant pas de frontières, il est particulièrement important de respecter la vie privée. L'Union doit veiller à ce que le droit fondamental à la protection des données soit appliqué systématiquement. Nous devons durcir la position de l'UE en matière de protection des données à caractère personnel dans le cadre de toutes les politiques européennes, y compris dans les domaines répressif et de la prévention de la criminalité, ainsi que dans nos relations internationales».*

Dans sa communication intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne»[7], 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.

Le champ d'application de la décision-cadre 2008/977/JAI est limité, car celle-ci s'applique uniquement aux traitements transfrontières de données, et non aux traitements effectués par les autorités policières et judiciaires au niveau strictement national. Cet état de droit est susceptible de causer des difficultés à la police et aux autres autorités compétentes dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière. Elles ne sont, en effet, pas toujours en mesure de distinguer aisément le traitement strictement national du traitement transfrontière, ni de prévoir si certaines données à caractère personnel pourraient faire l'objet d'un échange transfrontière à un stade ultérieur (voir section 2 ci-après). Par sa nature et son contenu, la décision-cadre confère en outre aux États membres une très grande marge de manœuvre pour transposer ses dispositions en droit national. Qui plus est, cette décision ne prévoit aucun mécanisme ni aucun groupe consultatif analogue au groupe de travail «Article 29» favorisant l'interprétation commune de ses dispositions, ni aucune compétence d'exécution en faveur de la Commission pour garantir une approche commune de sa mise en œuvre.

L'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE) établit le principe selon lequel toute personne physique 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, qui s'applique également à la coopération judiciaire en matière pénale et à la coopération policière. 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. L'article 16 du TFUE exige du législateur qu'il fixe des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel également dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière, couvrant le traitement, tant transfrontière que national, des données à caractère personnel. Ceci permettra de protéger les libertés et droits fondamentaux des personnes physiques, et notamment leur droit à la protection des données à caractère personnel, tout en assurant l'échange de ces données 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, ce qui contribuera également à faciliter la coopération dans la lutte contre la criminalité en Europe.

---

[7] Commission européenne, communication relative à «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», COM(2010)609 final du 4 novembre 2010.

En raison de la nature spécifique des domaines de la coopération judiciaire en matière pénale et de la coopération policière, il a été reconnu dans la déclaration 21[8] annexée au TFUE que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation de ces données dans ces domaines, se basant sur l'article 16 du TFUE, pourraient s'avérer nécessaires.

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 pris la forme 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. Les contributions non confidentielles peuvent être consultées sur le site internet de la Commission[9];

– 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. Les contributions non confidentielles peuvent être consultées sur le site internet de la Commission[10].

Tandis que ces consultations ont essentiellement porté sur la révision de la directive 95/46/CE, des consultations ciblées ont été menées auprès des services répressifs; en particulier, un atelier a eu lieu le 29 juin 2010 avec les autorités des États membres sur l'application des règles de protection des données à caractère personnel aux autorités publiques, y compris dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale. En outre, le 2 février 2011, la Commission a organisé un atelier avec les autorités des États membres pour discuter de la mise œuvre de la décision-cadre 2008/977/JAI et, plus généralement, des questions de protection des données dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale.

Les citoyens de l'Union ont été consultés dans le cadre d'une enquête Eurobaromètre qui s'est déroulée aux mois de novembre et décembre 2010[11]. Plusieurs études ont également été entreprises[12]. Le groupe de travail «Article 29»[13] a rendu plusieurs avis et apporté une

---

8 Déclaration 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière (annexée à l'acte final de la Conférence intergouvernementale qui a adopté le traité de Lisbonne le 13.12.2007).

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

10 http://ec.europa.eu/justice/newsroom/data-protection/events/101104_en.htm (en anglais uniquement).

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).

12 Voir l'*Étude sur les avantages économiques des technologies renforçant la protection de la vie privée* ou 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).

contribution utile à la Commission[14]. 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[15].

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[16]. 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 dans tous les États membres[17].

Conformément à sa politique tendant à «mieux légiférer», la Commission a réalisé une analyse d'impact des différentes options possibles[18]. 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. En ce qui concerne ce dernier objectif en particulier, deux options ont été analysées: une première option étendant simplement la portée des règles de protection des données à ce domaine et remédiant aux lacunes et autres questions soulevées par la décision-cadre, et une seconde option plus complète, assortie de règles extrêmement normatives et strictes, qui impliquerait en outre la modification immédiate de tous les autres instruments relevant de «l'ancien troisième pilier». Une option «minimaliste» largement fondée sur des communications interprétatives et des mesures de soutien telles que des programmes de financement et des instruments techniques, avec une intervention législative minimale, n'a pas été jugée appropriée pour remédier aux problèmes recensés dans ce domaine en rapport avec la protection des données.

---

13 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.

14 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 95/46/CE. Ces documents peuvent tous être consultés à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm

15 Elle est disponible sur le site internet du CEDP: http://www.edps.europa.eu/EDPSWEB/.

16 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).

17 CESE 999/2011.

18 SEC(2012) 72.

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 intégrée dans la présente proposition. D'après l'analyse d'impact, la mise en œuvre de cette option devrait permettre de renforcer encore la protection des données dans ce domaine, notamment par l'inclusion des traitements de données nationaux, et ainsi d'accroître la sécurité juridique pour les autorités compétentes dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière.

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.

La Commission a également établi un rapport sur la mise en œuvre de la décision-cadre 2008/977/JAI, au titre de son article 29, paragraphe 2, qui devrait être adopté dans le cadre du présent train de mesures sur la protection des données[19]. Les conclusions du rapport, fondées sur les informations fournies par les États membres, ont également été intégrées à la préparation de l'analyse d'impact.

3. ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

3.1. Base juridique

La présente proposition est fondée sur l'article 16, paragraphe 2, du TFUE, qui est la nouvelle base juridique spécifique, introduite par le traité de Lisbonne, pour l'adoption de règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, ainsi que de règles relatives à la libre circulation de ces données.

La proposition vise à garantir un niveau homogène et élevé de protection des données dans ce domaine, favorisant ainsi la confiance mutuelle entre les autorités policières et judiciaires des divers États membres et facilitant la libre circulation des données et la coopération entre ces mêmes services.

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

[19] COM(2012) 12.

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 dans les domaines de la police et de la justice pénale 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 et à l'article 16, paragraphe 1, du TFUE, exige un niveau de protection des données identique dans l'ensemble de l'Union. Il requiert le même niveau de protection pour les données échangées et traitées au niveau national.

– Il devient de plus en plus nécessaire que les services répressifs nationaux puissent traiter et échanger plus rapidement des données afin de prévenir et de combattre la criminalité transnationale et le terrorisme. Dans ce contexte, des règles claires et cohérentes en matière de protection des données au niveau de l'UE contribueront à développer la coopération entre les services concernés.

– 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 de garantir une application uniforme du droit de l'Union. Dans certaines situations, l'Union européenne est 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 ont de fortes chances d'être 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 la rédaction de celle-ci.

Une directive est donc l'instrument le plus adéquat pour garantir une harmonisation au niveau de l'UE dans ce domaine, tout en laissant aux États membres la souplesse nécessaire dans la mise en œuvre de ces règles et principes ainsi que de leurs dérogations à l'échelle nationale. Compte tenu de la complexité des règles nationales actuelles relatives à la protection des données à caractère personnel traitées dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, ainsi que de l'objectif d'harmonisation globale de ces règles par voie de directive, la Commission devra demander aux États membres de lui fournir des documents expliquant le lien entre les éléments de la directive et les parties

correspondantes des instruments nationaux de transposition, afin de pouvoir accomplir la mission dont elle est investie de veiller à la transposition de la présente directive.

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 des droits fondamentaux 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[20], 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[21]. 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 par la charte et pouvant être affectés sont 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) et le droit à un recours effectif et à accéder à un tribunal impartial (article 47).

3.4. Explication détaillée de la proposition

3.4.1. CHAPITRE I - DISPOSITIONS GÉNÉRALES

L'article 1er définit l'objet de la directive, à savoir l'établissement de règles relatives au traitement de données à caractère personnel 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 énonce les deux objectifs poursuivis par ce texte: protéger les libertés et droits fondamentaux des personnes physiques, et notamment leur droit à la protection des données à caractère personnel, et assurer l'échange de ces données entre autorités compétentes au sein de l'Union.

L'article 2 définit le champ d'application de la directive, qui ne se limite pas au traitement transfrontière de données, mais s'applique à l'ensemble des traitements effectués par les «autorités compétentes» (définies à l'article 3, paragraphe 14, aux fins de la directive). La directive ne s'applique ni aux traitements effectués au cours des activités ne relevant pas du champ d'application du droit de l'Union ni à ceux réalisés par les institutions, organes, et organismes de l'Union, qui font l'objet du règlement (CE) n° 45/2001 et d'une législation spécifique.

L'article 3 définit des termes employés dans la directive. Si certaines définitions sont reprises de la directive 95/46/CE ou de la décision-cadre 2008/977/JAI, d'autres sont modifiées ou

---

20 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.

21 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.

complétées par des éléments supplémentaires, ou sont nouvelles. Les nouvelles définitions sont celles des termes et expressions suivants: «violation de données à caractère personnel», «données génétiques» et «données biométriques», «autorités compétentes» [cette dernière définition est fondée sur l'article 87 du TFUE et l'article 2, point h), de la décision-cadre 2008/977/JAI] et «enfant», définition fondée sur la convention des Nations unies relative aux droits de l'enfant[22].

3.4.2. CHAPITRE II - PRINCIPES

L'article 4 énonce les principes régissant le traitement des données à caractère personnel; il s'inspire de l'article 6 de la directive 95/46/CE et de l'article 3 de la décision-cadre 2008/977/JAI, tout en adaptant ces principes au contexte particulier de la présente directive.

L'article 5 oblige les États membres à établir, dans la mesure du possible, une distinction entre les données à caractère personnel de différentes catégories de personnes concernées. Il constitue une disposition nouvelle qui ne figure ni dans la directive 95/46/CE ni dans la décision-cadre 2008/977/JAI, mais que la Commission avait insérée dans sa proposition initiale de décision-cadre[23]. Il s'inspire de la recommandation n° R (87)15 du Conseil de l'Europe. Il existe déjà des règles similaires pour Europol[24] et Eurojust[25].

L'article 6 relatif aux niveaux de précision et de fiabilité des données à caractère personnel s'inspire du principe 3.2 de la recommandation n° R (87)15 du Conseil de l'Europe. Il existe des règles similaires pour Europol[26], qui figurent également dans la proposition de décision-cadre présentée par la Commission.

L'article 7 énonce les motifs fondant la licéité du traitement: celui-ci doit être nécessaire à l'exécution d'une mission par une autorité compétente en vertu de la législation nationale, au respect d'une obligation légale à laquelle le responsable du traitement est soumis, à la sauvegarde des intérêts vitaux de la personne concernée, ou pour prévenir une menace grave et immédiate pour la sécurité publique. Les autres motifs fondant la licéité du traitement visés à l'article 7 de la directive 95/46/CE ne sont pas pertinents aux fins du traitement dans le domaine de la police et de la justice pénale.

L'article 8, inspiré 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

---

22 Mentionné également à l'article 2, point a), de la directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, JO L 335 du 17.12.2011, p. 1.

23 COM(2005) 475 final.

24 Article 14 de la décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol).

25 Article 15 de la décision 2009/426/JAI du Conseil du 16 décembre 2008 sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité.

26 Article 14 de la décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol).

exceptions à cette règle générale; il ajoute à ces catégories celle des données génétiques, conformément à la jurisprudence de la Cour européenne des droits de l'homme[27].

L'article 9 interdit les mesures exclusivement fondées sur un traitement automatisé de données à caractère personnel, à moins qu'elles ne soient autorisées par une loi prévoyant des garanties appropriées, dans le sens de l'article 7 de la décision-cadre 2008/977/JAI.

3.4.3. CHAPITRE III - DROITS DE LA PERSONNE CONCERNÉE

L'article 10 introduit l'obligation, pour les États membres, 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[28], et d'imposer aux responsables du traitement de prévoir des procédures et des mécanismes permettant aux personnes concernées d'exercer leurs droits plus aisément. Ces procédures et mécanismes comprennent notamment l'obligation de prévoir l'exercice, en principe gratuit, de ces droits.

L'article 11 énonce l'obligation incombant aux États membres de veiller à l'information de la personne concernée. Ces obligations se situent dans le prolongement des articles 10 et 11 de la directive 95/46/CE, sans que des articles distincts ne précisent si les informations sont ou non collectées auprès de la personne concernée; elles élargissent ainsi les informations à fournir. Cet article prévoit également des exceptions à l'obligation d'information lorsque celles-ci sont nécessaires et proportionnées dans une société démocratique à l'exercice des tâches des autorités compétentes (voir article 13 de la directive 95/46/CE et article 17 de la décision-cadre 2008/977/JAI).

L'article 12 oblige les États membres à garantir à la personne concernée un droit d'accès aux données à caractère personnel la concernant. Il reprend 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 ou à l'effacement, ou de demander la limitation du traitement, et de leur droit de réclamation.

L'article 13, inspiré de l'article 17, paragraphes 2 et 3, de la décision-cadre 2008/977/JAI, dispose que les États membres peuvent adopter des mesures législatives limitant le droit d'accès si la nature spécifique du traitement des données dans les domaines de la police et de la justice pénale l'exige, ou prévoyant la communication à la personne concernée de la limitation d'accès.

L'article 14 introduit la règle selon laquelle, dans les cas où l'accès direct est limité, la personne concernée doit être informée de la possibilité de consulter indirectement les données, par l'intermédiaire de l'autorité de contrôle, qui devrait exercer ce droit pour le compte de ladite personne et est tenue de l'informer des résultats de ses vérifications.

L'article 15 sur le droit à la rectification reprend l'article 12, point b), de la directive 95/46/CE et, en ce qui concerne les obligations imposées en cas de refus, l'article 18, paragraphe 1, de la décision-cadre 2008/977/JAI.

---

[27] Arrêt de la Cour européenne des droits de l'homme du 4.12.2008, A. et Marper c. Royaume-Uni (Requêtes n^{os} 30562/04 et 30566/04).

[28] Adoptée, le 5 novembre 2009, par la conférence internationale des commissaires à la protection des données et de la vie privée.

L'article 16 sur le droit à l'effacement reprend l'article 12, point b), de la directive 95/46/CE et, en ce qui concerne les obligations imposées en cas de refus, l'article 18, paragraphe 1, de la décision-cadre 2008/977/JAI. Il intègre également le droit au marquage des données dans certains cas, en évitant le terme ambigu de «verrouillage» employé à l'article 12, point b), de la directive 95/46/CE et à l'article 18, paragraphe 1, de la décision-cadre 2008/977/JAI.

L'article 17 relatif à la rectification, l'effacement et la limitation du traitement dans les procédures judiciaires apporte des précisions fondées sur l'article 4, paragraphe 4, de la décision-cadre 2008/977/JAI.

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

3.4.4.1. SECTION 1 - OBLIGATIONS GÉNÉRALES

L'article 18 décrit les obligations incombant au responsable du traitement pour se conformer à la présente directive et en assurer le respect, notamment par l'adoption de règles internes et de mécanismes à cet effet.

L'article 19 dispose que les États membres doivent faire en sorte que le responsable du traitement respecte les obligations qui découlent des principes de protection des données dès la conception et de protection des données par défaut.

L'article 20 relatif aux responsables conjoints du traitement précise le statut de ces derniers en ce qui concerne leurs relations internes.

L'article 21 précise la fonction de sous-traitant et les obligations qui y sont attachées. Il reprend partiellement 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 manière autre que celle prévue dans les instructions du responsable du traitement doit être considéré comme responsable conjoint du traitement.

L'article 22 relatif aux traitements effectués sous l'autorité du responsable du traitement et du sous-traitant reprend l'article 16 de la directive 95/46/CE.

L'article 23 introduit l'obligation, pour les responsables du traitement et les sous-traitants, de conserver une trace documentaire de tous les systèmes et procédures de traitement sous leur responsabilité.

L'article 24 est relatif à l'établissement de relevés, conformément à l'article 10, paragraphe 1, de la décision-cadre 2008/977/JAI et apporte des précisions supplémentaires.

L'article 25 précise les obligations qui incombent au responsable du traitement et au sous-traitant dans le cadre de leur coopération avec l'autorité de contrôle.

L'article 26, inspiré de l'article 23 de la décision-cadre 2008/977/JAI, vise les cas dans lesquels une consultation de l'autorité de contrôle est obligatoire préalablement au traitement.

3.4.4.2. SECTION 2 - SÉCURITÉ DES DONNÉES

L'article 27 relatif à la sécurité des traitements et inspiré de l'actuel article 17, paragraphe 1, de la directive 95/46/CE concernant la sécurité des traitements, ainsi que de l'article 22 de la

décision-cadre 2008/977/JAI, étend aux sous-traitants les obligations correspondantes, quelle que soit la nature du contrat qu'ils ont conclu avec le responsable du traitement.

Les articles 28 et 29 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»); ils précisent et distinguent, d'une part, l'obligation de notification à l'autorité de contrôle (article 28) et, d'autre part, l'obligation d'information, dans certaines circonstances, de la personne concernée (article 29). L'article 29 prévoit aussi des dérogations fondées sur les motifs énumérés à l'article 11, paragraphe 4.

3.4.4.3. SECTION 3 - DÉLÉGUÉ À LA PROTECTION DES DONNÉES

L'article 30 introduit l'obligation, à la charge du responsable du traitement, de désigner un délégué à la protection des données chargé des missions énumérées à l'article 32. Lorsque plusieurs autorités compétentes agissent sous le contrôle d'une autorité centrale, faisant office de responsable du traitement, il devrait incomber au moins à cette autorité centrale de désigner ce délégué. L'article 18, paragraphe 2, de la directive 95/46/CE prévoyait la possibilité pour les États membres d'introduire une telle obligation à la place de l'obligation de notification générale imposée par ladite directive.

L'article 31 définit la fonction du délégué à la protection des données.

L'article 32 prévoit les missions du délégué à la 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 33 énonce les principes généraux applicables aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, y compris les transferts ultérieurs. Il précise que les transferts vers des pays tiers ne peuvent avoir lieu que s'ils sont nécessaires 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.

L'article 34 autorise les transferts vers un pays tiers pour lequel la Commission a adopté une décision constatant le caractère adéquat du niveau de protection en vertu du règlement …./../201X ou ceux relevant spécifiquement du domaine de la coopération policière et de la coopération judiciaire en matière pénale ou, en l'absence d'une telle décision, lorsqu'il existe des garanties appropriées. Tant qu'aucune décision constatant le caractère adéquat du niveau de protection n'a été adoptée, la directive fait en sorte que les transferts puissent se poursuivre sur le fondement de garanties appropriées et de dérogations. Elle énonce en outre les critères permettant à la Commission d'apprécier le caractère adéquat ou non d'un niveau de protection, et inclut expressément la primauté du droit, l'existence d'un droit de recours judiciaire et un contrôle indépendant. Cet article prévoit également la faculté pour 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. Il ajoute qu'une décision générale relative au caractère adéquat du niveau de protection, adoptée selon les procédures prévues à l'article 38 du règlement général sur la protection des données, est applicable dans les limites de la présente directive. Il est également possible que la Commission adopte une telle décision aux fins exclusives de la présente directive.

L’article 35 définit les garanties appropriées qui, en l’absence d’une décision de la Commission relative au caractère adéquat du niveau de protection, sont exigées avant tout transfert international. Pareilles garanties peuvent être offertes par un instrument juridiquement contraignant tel qu’une convention internationale. Le responsable du traitement peut aussi, sur la base d’une évaluation des circonstances entourant le transfert, conclure à l’existence de ces garanties.

L'article 36 définit les dérogations autorisées pour les transferts de données, sur la base de l'article 26 de la directive 95/46/CE et de l'article 13 de la décision-cadre 2008/977/JAI.

L’article 37 oblige les États membres à prévoir que le responsable du traitement informe le destinataire de toute limitation du traitement et prend toutes les mesures raisonnables pour que ces limitations soient respectées par les destinataires des données à caractère personnel dans le pays tiers ou l’organisation internationale.

L'article 38 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.

CHAPITRE VI – AUTORITÉS DE CONTRÔLE INDÉPENDANTES

3.4.5.1. SECTION 1 - STATUT D’INDÉPENDANCE

Inspiré de l'article 28, paragraphe 1, de la directive 95/46/CE, et de l'article 25 de la décision-cadre 2008/977/JAI, l'article 39 fait obligation aux États membres de mettre en place des autorités de contrôle, et d'élargir la mission de celles-ci qui seront également chargées de contribuer à l'application cohérente de la directive dans l’ensemble de l'Union; cette autorité de contrôle peut être celle instituée en vertu du règlement général sur la protection des données.

L'article 40 clarifie les conditions garantissant l'indépendance des autorités de contrôle, en application de la jurisprudence de la Cour de justice de l'Union européenne[29], et en s'inspirant également de l'article 44 du règlement (CE) n° 45/2001[30].

L'article 41 énonce les conditions générales applicables aux membres de l’autorité de contrôle, en application de la jurisprudence en la matière[31], et en s'inspirant également de l'article 42, paragraphes 2 à 6, du règlement (CE) n° 45/2001.

L'article 42 définit les règles relatives à l’établissement de l'autorité de contrôle, y compris celles applicables à ses membres, que les États membres devront fixer par voie législative.

---

29 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.

30 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.

31 Op. cit., note de bas de page n° 27.

L’article 43 relatif au secret professionnel des membres et du personnel de l'autorité de contrôle s'inspire de l'article 28, paragraphe 7, de la directive 95/46/CE et de l’article 25, paragraphe 4, de la décision-cadre 2008/977/JAI.

3.4.5.2. SECTION 2 - FONCTIONS ET POUVOIRS

L'article 44, inspiré de l'article 28, paragraphe 6, de la directive 95/46/CE et de l’article 25 de la décision-cadre 2008/977/JAI, définit la compétence des autorités de contrôle. Lorsqu'elles agissent en leur qualité de pouvoir judiciaire, 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 45 fait obligation aux États membres de définir 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. Une fonction propre aux autorités de contrôle dans le contexte de la présente directive consiste, lorsque l'accès direct aux données est refusé ou limité, à exercer le droit d'accès pour le compte des personnes concernées et à vérifier la licéité du traitement de ces données.

L'article 46, inspiré de l'article 28, paragraphe 3, de la directive 95/46/CE et de l'article 25, paragraphes 2 et 3 de la décision-cadre 2008/977/JAI, énonce les pouvoirs de l'autorité de contrôle. L'article 47 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.

3.4.6. CHAPITRE VII – COOPÉRATION

L'article 48 instaure des règles en matière d'assistance mutuelle obligatoire alors que l'article 28, paragraphe 6, deuxième alinéa, de la directive 95/46/CE se bornait à prévoir une obligation générale de coopération, sans autre précision.

L'article 49 prévoit que le comité européen de la protection des données, institué par le règlement général sur la protection des données, exerce ses missions dans le contexte également des traitements relevant du champ d'application de la présente directive. Afin de fournir un appui complémentaire, la Commission sollicitera l’avis des représentants des autorités nationales compétentes en matière de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière, ainsi que celui des représentants d’Europol et d’Eurojust, au moyen d’un groupe d’experts sur les aspects répressifs de la protection des données.

3.4.7. CHAPITRE VIII – VOIES DE RECOURS, RESPONSABILITÉ ET SANCTIONS

L'article 50 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, et vise toute infraction à la directive en rapport avec l’auteur de la réclamation. 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 51 concerne le droit à 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 expressément que la personne concernée peut intenter une action en justice pour contraindre une autorité de contrôle à donner suite à une réclamation.

L'article 52, s'appuyant sur l'article 22 de la directive 95/46/CE et sur l'article 20 de la décision-cadre 2008/977/JAI, concerne le droit de former un recours juridictionnel contre un responsable du traitement ou un sous-traitant.

L'article 53 instaure 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 et le droit des autorités de contrôle d'ester en justice. L'obligation incombant aux États membres de veiller à ce que les actions en justice permettent l'adoption rapide de mesures est inspirée de l'article 18, paragraphe 1, de la directive 2000/31/CE sur le commerce électronique[32].

L'article 54 fait obligation aux États membres de prévoir un droit à réparation. S'appuyant sur l'article 23 de la directive 95/46/CE et l'article 19, paragraphe 1, de la décision-cadre 2008/977/JAI, il étend ce droit aux dommages causés par les sous-traitants et clarifie la responsabilité des responsables conjoints du traitement et des sous-traitants assurant conjointement le traitement.

L'article 55 oblige les États membres à définir les sanctions pénales applicables aux infractions à la directive, et à veiller à l'application desdites sanctions.

3.4.8. CHAPITRE IX - ACTES DÉLÉGUÉS ET ACTES D'EXÉCUTION

L'article 56 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 57 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.

3.4.9. CHAPITRE X - DISPOSITIONS FINALES

L'article 58 abroge la décision-cadre 2008/977/JAI.

L'article 59 prévoit que les dispositions spécifiques concernant le 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, figurant dans des actes de l'Union, régissant le traitement des données à caractère personnel ou l'accès aux systèmes d'information relevant du champ d'application de la directive, et adoptées avant l'adoption de la présente directive, demeurent inchangées.

L'article 60 clarifie la relation de la présente directive avec les accords internationaux conclus antérieurement par les États membres dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière.

---

[32] 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 61 fait obligation à la Commission d’évaluer la transposition de la directive et d’en rendre compte, afin d'apprécier la nécessité d'harmoniser avec celle-ci les dispositions spéciales antérieurement adoptées, énoncées à l’article 59.

L'article 62 impose aux États membres de transposer la directive dans leur droit national et de notifier à la Commission les dispositions adoptées en vertu de la directive.

L'article 63 fixe la date d'entrée en vigueur de la directive.

L'article 64 désigne les destinataires de la directive.

4. INCIDENCES BUDGÉTAIRES

La fiche financière législative accompagnant la proposition de règlement couvre les incidences budgétaires du règlement et de la présente directive.

2012/0010 (COD)

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

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

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

vu la proposition de la Commission européenne,

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

après consultation du contrôleur européen de la protection des données[33],

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.

(3) 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 aux autorités compétentes d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités.

[33] JO C… du …, p. ….

(4) Cette évolution exige de faciliter la libre circulation des données entre les autorités compétentes 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. Cela oblige à mettre en place dans l'Union un cadre de protection des données solide et plus cohérent, assorti d'une application rigoureuse des règles.

(5) 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[34] s'applique à l'ensemble des activités de traitement des données à caractère personnel dans les États membres, à la fois dans les secteurs public et privé. Elle ne s'applique cependant pas au traitement de données à caractère personnel mis en œuvre «pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire», telles que les activités dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière.

(6) La 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[35] s'applique dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière. Son champ d'application se borne au traitement des données à caractère personnel qui sont transmises ou mises à disposition entre les États membres.

(7) Il est crucial d'assurer un niveau élevé et homogène de protection des personnes physiques et de faciliter l'échange de données à caractère personnel entre les autorités compétentes des États membres, afin de garantir l'efficacité de la coopération judiciaire en matière pénale et de la coopération policière. À cette fin, le niveau de protection des droits et libertés 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, devrait être équivalent dans tous les États membres. Une protection effective des données à caractère personnel dans toute l'Union exige non seulement de renforcer les droits des personnes concernées et les obligations de ceux qui traitent ces données, 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.

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

(9) Sur cette base, le règlement (UE) …../2012 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) définit des règles générales visant à protéger les personnes

---

34 JO L 281 du 23.11.1995, p. 31.

35 JO L 350 du 30.12.2008, p. 60.

physiques à l'égard du traitement des données à caractère personnel et à garantir la libre circulation de ces données dans l'Union.

(10) Dans la déclaration 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, annexée à l'acte final de la Conférence intergouvernementale qui a adopté le traité de Lisbonne, la Conférence a reconnu que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation de ces données dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière se basant sur l'article 16 du traité sur le fonctionnement de l'Union européenne pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines.

(11) Par conséquent, une directive distincte devrait permettre de répondre à la nature spécifique de ces domaines et de fixer les règles relatives 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.

(12) Afin d'assurer le même niveau de protection pour les personnes physiques au moyen de droits juridiquement protégés à travers l'Union et d'éviter que des différences n'entravent les échanges de données à caractère personnel entre les autorités compétentes, la directive devrait prévoir des règles harmonisées pour la protection et la libre circulation des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière.

(13) La présente directive permet de prendre en compte, dans la mise en œuvre de ses dispositions, le principe du droit d'accès du public aux documents administratifs.

(14) La protection conférée par la présente directive devrait concerner les personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, dans le cadre du traitement des données à caractère personnel.

(15) 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 de la présente directive. La présente directive ne devrait s'appliquer ni au traitement de données à caractère personnel s'inscrivant dans le cadre d'activités ne relevant pas du champ d'application du droit de l'Union, notamment celles relatives à la sûreté de l'État, ni à celui effectué par les institutions, organes, et organismes de l'Union, tels qu'Europol ou Eurojust.

(16) Il y a lieu d'appliquer les principes de protection à toute information concernant une personne physique identifiée ou identifiable. Pour déterminer si une personne physique 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.

(17) 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 la source, provenant 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.

(18) Tout traitement de données à caractère personnel devrait être loyal et licite à l'égard des personnes concernées. En particulier, les finalités spécifiques du traitement devraient être explicites.

(19) Aux fins de la prévention des infractions pénales, et des enquêtes et poursuites en la matière, les autorités compétentes ont besoin de conserver et de traiter des données à caractère personnel, collectées dans le contexte de la prévention et de la détection d'infractions pénales spécifiques, et des enquêtes et poursuites en la matière et, au-delà de ce contexte, pour acquérir une meilleure compréhension des phénomènes criminels et des tendances qui les caractérisent, recueillir des renseignements sur les réseaux criminels organisés et établir des liens entre les différentes infractions mises au jour.

(20) Des données à caractère personnel ne devraient pas être traitées à des fins incompatibles avec la finalité pour laquelle elles ont été collectées. Les données à caractère personnel traitées devraient être adéquates, pertinentes et non excessives au regard des finalités du traitement. Il y a lieu de prendre toutes les mesures raisonnables afin que les données à caractère personnel qui sont inexactes soient rectifiées ou effacées.

(21) Il conviendrait d'appliquer le principe d'exactitude des données en tenant compte de la nature et de l'objet du traitement concerné. Dans le cadre des procédures judiciaires, notamment, les déclarations contenant des données à caractère personnel sont, en effet, fondées sur des perceptions personnelles subjectives et ne sont pas toujours vérifiables. Ce principe ne devrait donc pas s'appliquer à l'exactitude de la déclaration elle-même mais simplement au fait qu'une certaine déclaration a été faite.

(22) Dans l'interprétation et l'application des principes généraux relatifs au 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, il convient de tenir compte des particularités du domaine, y compris des objectifs spécifiques poursuivis.

(23) Le traitement des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière implique nécessairement le traitement de données à caractère personnel concernant différentes catégories de

personnes. Il importe donc d'établir une distinction aussi claire que possible entre les données à caractère personnel concernant différentes catégories de personnes, telles que les suspects, les personnes reconnues coupables d'une infraction pénale, les victimes et les tiers, tels que les témoins, les personnes détenant des informations ou des contacts utiles, et les complices de personnes soupçonnées ou condamnées.

(24) Il conviendrait, dans la mesure du possible, de différencier les données à caractère personnel en fonction de leur degré d'exactitude et de fiabilité. Il y aurait lieu de distinguer les faits des appréciations personnelles, afin de garantir à la fois la protection des personnes physiques et la qualité et la fiabilité des informations traitées par les autorités compétentes.

(25) Pour être licite, le traitement des données à caractère personnel devrait être nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, à l'exécution d'une mission d'intérêt général par une autorité compétente, prévue par la législation, à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne, ou à la prévention d'une menace grave et immédiate pour la sécurité publique.

(26) Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des droits fondamentaux et de la vie privée, notamment les données génétiques, méritent une protection spécifique. Ces données ne devraient pas faire l'objet d'un traitement, à moins que celui ne soit spécifiquement autorisé par une loi prévoyant des mesures appropriées de sauvegarde des intérêts légitimes de la personne concernée; qu'il ne soit nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne; ou qu'il ne porte sur des données manifestement rendues publiques par la personne concernée.

(27) Toute personne physique devrait avoir le droit de ne pas être soumise à une mesure fondée exclusivement sur un traitement automatisé si cette dernière produit des effets juridiques défavorables pour elle, à moins que la mesure ne soit autorisée par la loi et subordonnée à des mesures appropriées de sauvegarde des intérêts légitimes de la personne concernée.

(28) Afin de permettre aux personnes concernées d'exercer leurs droits, toute information leur étant destinée devrait être aisément accessible et facile à comprendre, et notamment formulée en termes simples et clairs.

(29) Des modalités devraient être prévues pour faciliter l'exercice par la personne concernée des droits qui lui sont conférés par la présente directive, notamment les moyens de demander sans frais l'accès aux données, leur rectification ou leur effacement. Le responsable du traitement devrait être tenu de répondre aux demandes de la personne concernée sans retard indu.

(30) Le principe de traitement loyal 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.

(31) 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, au moment de leur enregistrement ou dans un délai raisonnable, après la collecte, eu égard aux circonstances particulières du traitement.

(32) 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, ainsi que l'identité des destinataires, y compris dans des pays tiers. Les personnes concernées devraient pouvoir obtenir une copie de leurs données personnelles faisant l'objet d'un traitement.

(33) Les États membres devraient être autorisés à adopter des mesures législatives visant à retarder ou à limiter l'information des personnes concernées ou leur accès aux données à caractère personnel les concernant, ou à ne pas leur accorder cette information ou cet accès, dès lors qu'une telle limitation partielle ou complète représente une mesure nécessaire et proportionnée dans une société démocratique, compte dûment tenu des intérêts légitimes de la personne concernée, afin d'éviter que des recherches, enquêtes ou procédures officielles ou légales ne soient entravées, d'éviter de nuire à la prévention et à la détection des infractions pénales, aux enquêtes et poursuites en la matière, ou à l'exécution de sanctions pénales, ou afin de protéger la sécurité publique ou la sûreté de l'État, ou de protéger la personne concernée ou les droits et libertés d'autrui.

(34) Tout refus d'accès ou toute limitation de celui-ci devrait être présenté par écrit à la personne concernée, en indiquant les motifs factuels ou juridiques sur lesquels la décision est fondée.

(35) Lorsqu'un État membre a adopté des mesures législatives limitant entièrement ou partiellement le droit d'accès, la personne concernée devrait avoir le droit de demander à l'autorité de contrôle nationale compétente de vérifier la licéité du traitement. La personne concernée devrait être informée de ce droit. Lorsque le droit d'accès est exercé par l'autorité de contrôle au nom de la personne concernée, l'autorité contrôle devrait au moins informer cette dernière que toutes les vérifications nécessaires ont été effectuées et de sa conclusion concernant la licéité du traitement en question.

(36) Toute personne devrait avoir le droit de faire rectifier des données à caractère personnel inexactes la concernant, et disposer d'un «droit à l'oubli numérique» à leur égard lorsque le traitement n'est pas conforme aux principes généraux énoncés dans la présente directive. Lorsque les données à caractère personnel sont traitées dans le cadre d'une enquête judiciaire ou d'une procédure pénale, le droit à l'information, le droit d'accès, de rectification et d'effacement, et le droit de limitation du traitement peuvent être exercés conformément aux règles nationales de procédure pénale.

(37) 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. En particulier, le responsable du traitement devrait veiller à la conformité des opérations de traitement avec les règles adoptées conformément à la présente directive.

(38) La protection des droits et libertés des personnes concernées à l'égard du traitement des données à caractère personnel les concernant exige l'adoption de mesures techniques et organisationnelles appropriées, afin de satisfaire aux exigences prévues par la présente directive. Afin de garantir la conformité du traitement avec les dispositions adoptées en application de la présente directive, le responsable du traitement devrait adopter des règles internes et mettre en œuvre les mesures appropriées, respectant notamment les principes de protection des données dès la conception et de protection des données par défaut.

(39) La protection des droits et libertés des personnes concernées, de même que la responsabilité des responsables du traitement et de leurs sous-traitants, exige une répartition claire des responsabilités au titre de la présente directive, 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.

(40) Les activités de traitement devraient être consignées par le responsable du traitement ou le sous-traitant, afin de permettre un contrôle de la conformité du traitement avec la présente directive. 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. .

(41) Afin de garantir en amont une protection effective des droits et libertés des personnes concernées, le responsable du traitement ou le sous-traitant devrait, dans certains cas, consulter l'autorité de contrôle avant d'entamer le traitement.

(42) Une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer un dommage, notamment une atteinte à la réputation de 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 nationale compétente. Les personnes physiques dont les données à caractère personnel ou la vie privée 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 physique 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, consécutifs au traitement des données à caractère personnel.

(43) 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'abus. Par ailleurs, ces règles et procédures devraient tenir compte des intérêts légitimes des autorités compétentes dans les cas où une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances de la violation.

(44) Le responsable du traitement ou le sous-traitant devrait désigner une personne chargée de l'aider à contrôler la bonne application des dispositions adoptées en vertu de la présente directive. Un délégué à la protection des données peut être désigné

conjointement par plusieurs entités de l'autorité compétente. Les délégués à la protection des données doivent être en mesure d'accomplir leurs missions et obligations de manière effective et en toute indépendance.

(45) Les États membres devraient veiller à ce qu'un transfert vers un pays tiers n'ait lieu que s'il est nécessaire 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, et si le responsable du traitement dans le pays tiers ou dans l'organisation internationale est une autorité compétente au sens de la présente directive. Un transfert peut avoir lieu lorsque la Commission a décidé que le pays tiers ou l'organisation internationale en question garantit un niveau adéquat de protection, ou lorsque des garanties appropriées ont été offertes.

(46) 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.

(47) Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait 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.

(48) La Commission devrait également pouvoir 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, sauf lorsqu'il est fondé sur une convention internationale, des garanties appropriées ou une dérogation. Il y aurait lieu de prévoir des procédures de consultation entre la Commission et le pays tiers ou l'organisation internationale. Cependant, une telle décision de la Commission ne doit pas supprimer la possibilité d'effectuer des transferts sur le fondement de garanties appropriées ou d'une dérogation prévue par la directive.

(49) Les transferts qui ne sont pas fondés sur une décision constatant le caractère adéquat de la protection ne devraient être autorisés que lorsque des garanties appropriées ont été offertes dans un instrument juridiquement contraignant, assurant la protection des données à caractère personnel, ou lorsque le responsable du traitement ou le sous-traitant a évalué toutes les circonstances entourant le transfert ou la série de transferts de données et estime, au vu de cette évaluation, qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel. Lorsqu'il n'y a pas de motif d'autoriser le transfert, des dérogations devraient être permises si elles sont nécessaires à la sauvegarde des intérêt vitaux de la personne concernée ou d'une autre personne, à la préservation des intérêts légitimes de la personne concernée, si le droit de l'État membre qui transfère les données à caractère personnel le prévoit, ou si les dérogations sont indispensables à la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers, ou, dans certains cas, 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, ou, dans des cas particuliers, à la constatation, l'exercice ou la défense d'un droit en justice.

(50) 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 pour se protéger de l'utilisation ou la divulgation illicite de ces dernières. 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 ou par l'hétérogénéité des régimes juridiques. 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 avec leurs homologues étrangers.

(51) 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. Il appartiendrait aux autorités de contrôle de surveiller l'application des dispositions de la présente directive 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. À cet effet, il conviendrait que les autorités de contrôle coopèrent entre elles et avec la Commission.

(52) Les États membres peuvent confier à une autorité de contrôle déjà créée dans les États membres conformément au règlement (UE) …./2012 la responsabilité des missions qui incombent aux autorités nationales de contrôle à instituer conformément à la présente directive.

(53) Les États membres devraient avoir la possibilité d'instituer plusieurs autorités de contrôle pour s'aligner sur leur structure constitutionnelle, organisationnelle et administrative. Il conviendrait que chaque autorité de contrôle soit dotée de tous les moyens financiers et humains appropriés, ainsi que des locaux et des 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.

(54) 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.

(55) Bien que la présente directive 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 dans le cadre de leur fonction juridictionnelle, afin de préserver l'indépendance des juges dans l'exercice de leurs fonctions judiciaires. 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.

(56) Afin d'assurer la cohérence du contrôle et de l'application de la présente directive 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.

(57) 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.

(58) Les autorités de contrôle devraient se prêter mutuellement assistance dans l'exercice de leurs fonctions, afin d'assurer une application cohérente des dispositions adoptées conformément à la présente directive.

(59) Le comité européen de la protection des données institué par le règlement (UE) …/2012 devrait contribuer à l'application cohérente de la présente directive dans toute l'Union, notamment en conseillant la Commission et en favorisant la coopération des autorités de contrôle dans l'ensemble de l'Union.

(60) 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 la présente directive ne sont pas respectés, si l'autorité de contrôle ne donne pas suite à une réclamation ou si elle n'agit pas alors qu'une action est nécessaire pour protéger les droits de la personne concernée.

(61) 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 les concernant et qui est constitué(e) conformément au droit d'un État membre devrait avoir le droit d'introduire une réclamation ou d'exercer le droit de recours pour le compte de personnes concernées l'ayant mandaté(e) à cet effet, 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.

(62) 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.

(63) 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 de la présente directive.

(64) 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.

(65) Toute personne physique ou morale, soumise au droit privé ou au 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.

(66) Afin de remplir les objectifs de la présente directive, à savoir la protection des libertés et droits fondamentaux des personnes physiques, et en particulier de leur droit à la protection des données à caractère personnel, et pour garantir le libre échange de ces dernières par les autorités compétentes 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 devraient être délégué à la Commission. Concrètement, des actes délégués devraient être adoptés en ce qui concerne la notification des violations de données à caractère personnel à l'autorité de contrôle. 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.

(67) Afin de garantir des conditions uniformes pour la mise en œuvre de la présente directive en ce qui concerne la documentation tenue par les responsables du traitement et les sous-traitants, la sécurité du traitement, notamment en matière de normes de cryptage, la notification d'une violation des données à caractère personnel à l'autorité de contrôle, et le niveau adéquat de protection atteint par un pays tiers, un territoire ou un secteur de traitement des données dans ce pays tiers, ou une organisation internationale, il y aurait lieu de conférer des compétences d'exécution à la Commission. 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[36].

(68) La procédure d'examen devrait être appliquée pour l'adoption de mesures relatives à la documentation tenue par les responsables du traitement et les sous-traitants, à la sécurité du traitement, à la notification d'une violation des données à caractère personnel à l'autorité de contrôle, et au niveau adéquat de protection atteint par un pays tiers, un territoire ou un secteur de traitement des données dans ce pays tiers, ou une organisation internationale, puisque ces actes sont de portée générale.

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

---

[36] JO L 55 du 28.2.2011, p. 13.

(70) Étant donné que les objectifs de la présente directive, à savoir protéger les libertés et les droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données personnelles, et garantir le libre échange de ces dernières par les autorités compétentes au sein 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, la présente directive n'excède pas ce qui est nécessaire pour atteindre cet objectif,

(71) La décision-cadre 2008/977/JAI devrait être abrogée par la présente directive.

(72) Les dispositions spécifiques concernant le traitement des données à caractère personnel par les autorités compétentes aux fins de la prévention et de la détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou de l'exécution de sanctions pénales, mentionnées dans des actes de l'Union adoptés avant la date d'adoption de la présente directive, qui régissent le traitement de données à caractère personnel entre États membres ou l'accès d'autorités désignées des États membres aux systèmes d'information créés en vertu des traités, devraient demeurent inchangées. La Commission devrait évaluer la situation en ce qui concerne la relation entre la présente directive et les actes adoptés avant la date de son adoption, qui régissent le traitement des données à caractère personnel entre États membres ou l'accès d'autorités désignées des États membres aux systèmes d'information créés en vertu des traités, afin d'apprécier la nécessité de mettre ces dispositions spécifiques en conformité avec la présente directive.

(73) Afin d'assurer une protection exhaustive et cohérente des données à caractère personnel dans l'Union, il conviendrait de modifier les conventions et accords internationaux conclus par les États membres avant l'entrée en vigueur de la présente directive, pour les harmoniser avec cette dernière.

(74) La présente directive est sans préjudice des dispositions relatives à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, de la directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011[37].

(75) Conformément à l'article 6 bis du protocole sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Royaume-Uni ou l'Irlande ne sera pas lié par les règles fixées dans la présente directive lorsque le Royaume-Uni ou l'Irlande n'est pas lié par les règles qui régissent des formes de coopération judiciaire en matière pénale ou de coopération policière dans le cadre desquelles les dispositions fixées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne doivent être respectées.

(76) Conformément aux articles 2 et 2 bis du protocole sur la position du Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark n'est pas lié par la présente directive ni soumis à son

[37] JO L 335 du 17.12.2011, p. 1.

application. Étant donné que la présente directive développe l'acquis de Schengen, en vertu du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne, le Danemark décidera, conformément à l'article 4 dudit protocole, dans un délai de six mois après l'adoption de la présente directive, s'il transposera celle-ci dans son droit national.

(77) En ce qui concerne l'Islande et la Norvège, la présente directive constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, 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[38].

(78) En ce qui concerne la Suisse, la présente directive constitue un développement des dispositions de l'acquis de Schengen 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[39].

(79) En ce qui concerne le Liechtenstein, la présente directive constitue un développement des dispositions de l'acquis de Schengen 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[40].

(80) La présente directive respecte les droits fondamentaux et observe les principes reconnus par la Charte des droits fondamentaux de l'Union européenne, consacrés par le traité, et notamment le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel et le droit à un recours effectif et à un procès équitable. Les limitations apportées à ces droits sont conformes à l'article 52, paragraphe 1, de la charte car elles sont nécessaires pour répondre à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

(81) Conformément à la déclaration politique commune des États membres et de la Commission du 28 septembre 2011 sur les documents explicatifs, les États membres se sont engagés à joindre à la notification de leurs mesures de transposition, dans les cas où cela se justifie, un ou plusieurs documents expliquant le lien entre les éléments d'une directive et les parties correspondantes des instruments nationaux de transposition. En ce qui concerne la présente directive, le législateur considère que la transmission de ces documents se justifie.

(82) La présente directive ne saurait empêcher les États membres de mettre en oeuvre l'exercice des droits des personnes concernées en matière d'information, d'accès, de rectification, d'effacement et de limitation du traitement de leurs données à caractère

---

38 JO L 176 du 10.7.1999, p. 36.
39 JO L 53 du 27.2.2008, p. 52.
40 JO L 160 du 18.6.2011, p. 19.

personnel dans le cadre de poursuites pénales, et les éventuelles limitations de ces droits, dans leur législation nationale en matière de procédure pénale,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I
DISPOSITIONS GÉNÉRALES

Article premier
Objet et objectifs

1. La présente directive établit les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes aux fins de la prévention et de la détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou de l'exécution de sanctions pénales.

2. Conformément à la présente directive, les États membres:

   a) protègent les libertés et droits fondamentaux des personnes physiques, et notamment leur droit à la protection des données à caractère personnel; et

   b) veillent à ce que l'échange de données à caractère personnel par les autorités compétentes au sein de l'Union ne soit ni limité ni interdit 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

1. La présente directive s'applique au traitement de données à caractère personnel effectué par les autorités compétentes aux fins énoncées à l'article 1er, paragraphe 1.

2. La présente directive 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.

3. La présente directive ne s'applique pas au traitement de données à caractère personnel effectué:

   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.

Article 3
Définitions

Aux fins de la présente directive, 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 des identifiants 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, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation du traitement, l'effacement ou la destruction;

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

(5) «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;

(6) «responsable du traitement»: l'autorité publique compétente qui, seule 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;

(7) «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;

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

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

(14) «autorités compétentes»: toutes 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.

(15) «autorité de contrôle»: une autorité publique qui est instituée par un État membre conformément aux dispositions de l'article 39.

CHAPITRE II
PRINCIPES

Article 4
Principes relatifs au traitement des données à caractère personnel

Les États membres prévoient que les données à caractère personnel doivent être:

a) traitées loyalement et licitement;

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 non excessives au regard des finalités pour lesquelles elles sont traitées;

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

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées;

f) traitées sous la responsabilité du responsable du traitement, qui veille au respect des dispositions adoptées en vertu de la présente directive.

.

Article 5

Distinction entre différentes catégories de personnes concernées

1. Les États membres prévoient que le responsable du traitement établit, dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que:

   a) les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale;

   b) les personnes reconnues coupables d'une infraction pénale;

   c) les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale;

   d) les tiers à l'infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, ou une personne pouvant fournir des informations sur des infractions pénales, ou un contact ou un associé de l'une des personnes mentionnées aux points a) et b); et

   e) les personnes qui n'appartiennent à aucune des catégories susmentionnées.

Article 6

Niveaux de précision et de fiabilité des données à caractère personnel

1. Les États membres veillent à ce qu'une distinction soit établie, dans la mesure du possible, entre les différentes catégories de données à caractère personnel soumises à un traitement, selon leur niveau de précision et de fiabilité.

2. Les États membres veillent à ce que les données à caractère personnel fondées sur des faits soient, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles.

Article 7

Licéité du traitement

Les États membres prévoient que le traitement des données à caractère personnel n'est licite que si, et dans la mesure où, il est nécessaire:

(a) à l'exécution d'une mission par une autorité compétente, en vertu de la législation, pour les finalités énoncées à l'article 1er, paragraphe 1; ou

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

(c) à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne; ou

(d) pour prévenir une menace grave et immédiate pour la sécurité publique.

Article 8

Traitements portant sur des catégories particulières de données à caractère personnel

1. Les États membres interdisent 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 la vie sexuelle.

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

   a) le traitement est autorisé par une législation prévoyant des garanties appropriées; ou

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

   c) le traitement porte sur des données manifestement rendues publiques par la personne concernée.

Article 9

Mesures fondées sur le profilage et sur le traitement automatisé

1. Les États membres prévoient que les mesures produisant des effets juridiques défavorables pour la personne concernée ou l'affectant de manière significative et qui sont prises sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects personnels propres à cette personne sont interdites, à moins d'être autorisées par une loi qui prévoit également des mesures destinées à préserver les intérêts légitimes de la personne concernée.

2. Le traitement automatisé de données à caractère personnel destiné à évaluer certains aspects personnels propres à la personne concernée ne saurait être exclusivement fondé sur les catégories particulières de données à caractère personnel mentionnées à l'article 8.

CHAPITRE III

DROITS DE LA PERSONNE CONCERNÉE

Article 10

Modalités de l'exercice des droits de la personne concernée

1. Les États membres prévoient que le responsable du traitement prend toutes les mesures raisonnables afin d'appliquer 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. Les États membres prévoient que le responsable du traitement procède à toute 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.

3. Les États membres prévoient que le responsable du traitement prend toutes les mesures nécessaires afin d'établir les procédures d'information prévues à l'article 11 et les procédures d'exercice des droits des personnes concernées mentionnés aux articles 12 à 17.

4. Les États membres prévoient que le responsable du traitement informe, sans retard injustifié, la personne concernée des suites données sa demande.

5. Les États membres prévoient que les informations et les éventuelles mesures prises par le responsable du traitement à la suite d'une demande prévue aux paragraphes 3 et 4 sont gratuites. Lorsque les demandes sont abusives, notamment en raison de leur caractère répétitif, ou de la longueur ou du volume de la demande, le responsable du traitement peut exiger le paiement de frais pour fournir les informations ou pour prendre la mesure demandée, ou peut s'abstenir de prendre cette dernière. Dans ce cas, il incombe au responsable du traitement de prouver le caractère abusif de la demande.

Article 11
Informations à la personne concernée

1. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées, les États membres veillent à ce que le responsable du traitement prenne les mesures appropriées pour fournir à cette personne au moins les informations suivantes:

   a) l'identité et les coordonnées du responsable du traitement et du délégué à la protection des données;

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

   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, leur rectification, leur effacement ou la limitation de leur traitement;

   e) le droit d'introduire une réclamation auprès de l'autorité de contrôle prévue à l'article 39, et les coordonnées de ladite autorité;

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

   g) toute autre information, dans la mesure où elle est 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 traitées.

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. Le responsable du traitement fournit les informations visées au paragraphe 1:

   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 traitées.

4. Les États membres peuvent adopter des mesures législatives prévoyant le retardement ou la limitation de la fourniture des informations, ou leur non-fourniture, aux personnes concernées dans la mesure où, et aussi longtemps que, cette limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, compte étant dûment tenu des intérêts légitimes de la personne concernée:

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

   (b) pour éviter de nuire à la prévention, à la détection, à la recherche et à la poursuite d'infractions pénales, ou pour exécuter des sanctions pénales;

   (c) pour protéger la sécurité publique;

   (d) pour protéger la sûreté de l'État;

   (e) pour protéger les droits et libertés d'autrui.

5. Les États membres peuvent déterminer des catégories de traitements de données susceptibles de faire l'objet, dans leur intégralité ou en partie, des dérogations prévues au paragraphe 4.

Article 12
Droit d'accès de la personne concernée

1. Les États membres prévoient le droit pour la personne concernée d'obtenir confirmation du responsable du traitement 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 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 ces données, ou la limitation de leur traitement ;

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.

2. Les États membres prévoient le droit pour la personne concernée d'obtenir du responsable du traitement une copie des données à caractère personnel en cours de traitement.

Article 13
Limitations du droit d'accès

1. Les États membres peuvent adopter des mesures législatives limitant, entièrement ou partiellement, le droit d'accès de la personne concernée, dès lors qu'une telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, compte étant dûment tenu des intérêts légitimes de la personne concernée:

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

(b) pour éviter de nuire à la prévention, à la détection, à la recherche et à la poursuite d'infractions pénales, ou pour exécuter des sanctions pénales;

(c) pour protéger la sécurité publique;

(d) pour protéger la sûreté de l'État;

(e) pour protéger les droits et libertés d'autrui.

2. Les États membres peuvent, par voie législative, déterminer des catégories de traitement de données susceptibles de faire l'objet, dans leur intégralité ou en partie, des dérogations prévues au paragraphe 1.

3. Dans les situations prévues aux paragraphes 1 et 2, les États membres prévoient qu'en cas de refus ou de limitation de l'accès aux données, le responsable du traitement informe la personne concernée, par écrit, des motifs du refus, et des possibilités d'introduire une réclamation auprès de l'autorité de contrôle et de former un recours juridictionnel. Les motifs de fait ou de droit qui fondent la décision

peuvent être omis lorsque leur communication risque de compromettre l'un des objectifs énoncés au paragraphe 1.

4. Les États membres veillent à ce que le responsable du traitement conserve une trace documentaire des raisons pour lesquelles il a omis de communiquer les motifs de fait ou de droit fondant la décision.

Article 14
Modalités de l'exercice du droit d'accès

1. Les États membres prévoient le droit pour la personne concernée de demander que l'autorité de contrôle, notamment dans les cas mentionnés à l'article 13, vérifie la licéité du traitement.

2. L'État membre prévoit que le responsable du traitement informe la personne concernée de son droit de demander l'intervention de l'autorité de contrôle en vertu du paragraphe 1.

3. Lorsque le droit mentionné au paragraphe 1 est exercé, l'autorité de contrôle informe la personne concernée, à tout le moins, de la réalisation de toutes les vérifications nécessaires incombant à l'autorité et du résultat concernant la licéité du traitement en question.

Article 15
Droit à rectification

1. Les États membres prévoient le droit pour la personne concernée 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, notamment au moyen d'une déclaration rectificative, que les données à caractère personnel incomplètes soient complétées.

2. Les États membres prévoient qu'en cas de refus de rectification des données, le responsable du traitement informe la personne concernée, par écrit, des motifs du refus, et des possibilités d'introduire une réclamation auprès de l'autorité de contrôle et de former un recours juridictionnel.

Article 16
Droit à l'effacement

1. Les États membres prévoient le droit pour la personne concernée d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant lorsque le traitement n'est pas conforme aux dispositions adoptées conformément à l'article 4, points a) à e), à l'article 7 et à l'article 8 de la présente directive.

2. Le responsable du traitement procède à l'effacement sans délai.

3. Au lieu de procéder à l'effacement, le responsable du traitement marque les 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) lorsque les données à caractère personnel doivent être conservées à des fins probatoires;

   (c) lorsque la personne concernée s'oppose à leur effacement et exige, à la place de cela, la limitation de leur utilisation.

4. Les États membres prévoient que le responsable du traitement informe la personne concernée, par écrit, de tout refus d'effacer ou de marquer les données traitées, des motifs du refus, et des possibilités d'introduire une réclamation auprès de l'autorité de contrôle et de former un recours juridictionnel.

Article 17

Droits des personnes concernées lors des enquêtes et des procédures pénales

Les États membres peuvent prévoir que, lorsque les données à caractère personnel figurent dans une décision judiciaire ou un casier judiciaire faisant l'objet d'un traitement lors d'une enquête judiciaire ou d'une procédure pénale, les droits d'information, d'accès, de rectification, d'effacement et de limitation du traitement prévus aux articles 11 à 16 sont exercés conformément aux règles nationales de procédure pénale.

CHAPITRE IV
RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT

SECTION 1
OBLIGATIONS GÉNÉRALES

Article 18

Obligations incombant au responsable du traitement

1. Les États membres prévoient que le responsable du traitement adopte des règles internes et met en œuvre les mesures appropriées pour garantir que le traitement des données à caractère personnel sera effectué dans le respect des dispositions adoptées conformément à la présente directive.

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

   a) la tenue de la documentation visée à l'article 23;

   b) le respect de l'obligation de consultation préalable prévue à l'article 26;

   c) la mise en œuvre des exigences en matière de sécurité des données prévues à l’article 27;

d) la désignation d'un délégué à la protection des données en application de l'article 30.

3. Le responsable du traitement met en œuvre des mécanismes pour vérifier l'efficacité des mesures visées au paragraphe 1 du présent article. Sous réserve de la proportionnalité d'une telle mesure, des auditeurs indépendants internes ou externes procèdent à cette vérification.

Article 19

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

1. Les États membres prévoient que, compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, le responsable du traitement applique les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux dispositions adoptées conformément à la présente directive 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 les données à caractère personnel nécessaires aux finalités du traitement seront traitées.

Article 20

Responsables conjoints du traitement

Les États membres prévoient que, 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 doivent définir, par voie d'accord, leurs obligations respectives afin de se conformer aux dispositions adoptées conformément à la présente directive, notamment en ce qui concerne les procédures et mécanismes régissant l'exercice des droits de la personne concernée.

Article 21

Sous-traitant

1. Les États membres prévoient que le responsable du traitement, lorsque une opération de traitement est effectué pour son compte, doit choisir 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 dispositions adoptées conformément à la présente directive et garantisse la protection des droits de la personne concernée.

2. Les États membres prévoient que la réalisation de traitements en sous-traitance doit être régie par un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sur instruction du responsable du traitement, en particulier lorsque le transfert des données à caractère personnel utilisées est interdit.

3. 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 20.

Article 22

Traitements effectués sous l'autorité du responsable du traitement et du sous-traitant

Les États membres prévoient que 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, ou s'il y est obligé par la législation de l'Union ou d'un État membre.

Article 23

Documentation

1. Les États membres prévoient que chaque responsable du traitement et chaque sous-traitant conservent une trace documentaire de tous les systèmes et procédures de traitement 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;

   b) les finalités du traitement;

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

   d) les transferts de données vers un pays tiers ou à une organisation internationale, y compris leur identification respective.

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

Article 24

Établissement de relevés des opérations de traitement

1. Les États membres veillent à ce que des relevés soient établis au moins pour les opérations de traitement suivantes: la collecte, l'altération, la consultation, la communication, l'interconnexion ou l'effacement. Les relevés des opérations de consultation et de communication indiquent en particulier la finalité, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel.

2. Les relevés sont utilisés uniquement à des fins de vérification de la licéité du traitement des données, d'autocontrôle et de garantie de l'intégrité et de la sécurité des données.

Article 25
Coopération avec l'autorité de contrôle

1. Les États membres prévoient que le responsable du traitement et le sous-traitant coopèrent, sur demande, avec l'autorité de contrôle dans l'exécution de ses fonctions, en communiquant notamment toutes les informations dont elle a besoin à cet effet.

2. Lorsque l'autorité de contrôle exerce les pouvoirs qui lui sont conférés en vertu de l'article 46, points a) et b), le responsable du traitement et le sous-traitant répondent à l'autorité de contrôle dans un délai raisonnable. La réponse comprend une description des mesures prises et des résultats obtenus, compte tenu des observations formulées par l'autorité de contrôle.

Article 26
Consultation préalable de l'autorité de contrôle

1. Les États membres veillent à ce que le responsable du traitement ou le sous-traitant consulte l'autorité de contrôle avant le traitement de données à caractère personnel qui feront partie d'un nouveau fichier à créer, si:

   a) le traitement vise des catégories particulières de données mentionnées à l'article 8;

   b) en raison notamment de l'utilisation de nouveaux mécanismes, technologies ou procédures, le type de traitement présente des risques spécifiques pour les libertés et droits fondamentaux, notamment la protection des données à caractère personnel, des personnes concernées.

2. Les États membres peuvent prévoir que l'autorité de contrôle établit une liste des traitements devant faire l'objet d'une consultation préalable conformément au paragraphe 1.

SECTION 2
SÉCURITÉ DES DONNÉES

Article 27
Sécurité des traitements

1. Les États membres prévoient que 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. En ce qui concerne le traitement automatisé de données, chaque État membre prévoit que le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à:

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

(b) empêcher que des supports de données ne puissent être lus, copiés, modifiés ou enlevés par une personne non autorisée (contrôle des supports de données);

(c) empêcher l'introduction non autorisée de données dans le fichier, ainsi que toute inspection, modification ou effacement non autorisé de données à caractère personnel enregistrées (contrôle du stockage);

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

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

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

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

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

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

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

3. La Commission peut adopter, si nécessaire, des actes d'exécution afin de préciser les exigences prévues aux paragraphes 1 et 2 dans diverses situations, et notamment les normes de cryptage. Ces actes d'exécution sont adoptés conformément à la procédure d'examen prévue à l'article 57, paragraphe 2.

Article 28

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

1. Les États membres prévoient qu'en cas de violation de données à caractère personnel, le responsable du traitement en adresse notification à l'autorité de contrôle sans retard indu et, si possible, 24 heures au plus tard après en avoir pris connaissance. Lorsque

la notification a lieu après ce délai, le responsable du traitement fournit une justification à l'autorité de contrôle, sur demande.

2. Le sous-traitant alerte et informe le responsable du traitement immédiatement après avoir eu connaissance de 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 visé à l'article 30 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 éventuelles 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. Les États membres prévoient que 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 uniquemement les informations nécessaires à cette fin.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 56, 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 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 57, paragraphe 2.

Article 29

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

1. Les États membres prévoient que, 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 28, 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 28, 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 à caractère personnel 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. La communication à la personne concernée peut être retardée, limitée ou omise pour les motifs visés à l'article 11, paragraphe 4.

SECTION 3
DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Article 30
Désignation du délégué à la protection des données

1. Les États membres prévoient que le responsable du traitement ou le sous-traitant désigne un délégué à la protection des données.

2. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées de la législation et des pratiques en matière de protection des données, et de sa capacité à accomplir les tâches énumérées à l'article 32.

3. Le délégué à la protection des données peut être désigné pour plusieurs entités, compte tenu de la structure organisationnelle de l'autorité compétente.

Article 31
Fonction du délégué à la protection des données

1. Les États membres prévoient que le responsable du traitement ou le sous-traitant veille 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 veille à ce que le délégué à la protection des données soit doté des moyens d'accomplir les missions et obligations visées à l'article 32 de manière effective et en toute indépendance, et ne reçoive aucune instruction en ce qui concerne l'exercice de sa fonction.

Article 32

Missions du délégué à la protection des données

Les États membres prévoient que le responsable du traitement ou le sous-traitant confie 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 application des dispositions adoptées conformément à la présente directive, et conserver une trace documentaire de cette activité et des réponses reçues;

(b) contrôler la mise en œuvre et l'application des règles internes 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 des dispositions adoptées conformément à la présente directive, 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 des dispositions adoptées conformément à la présente directive;

(d) veiller à ce que la documentation visée à l'article 23 soit tenue à jour;

(e) contrôler la documentation, la notification et la communication, prévues aux articles 28 et 29, et relatives aux violations de données à caractère personnel;

(f) vérifier que les demandes d'autorisation ou de consultation préalables ont été introduites, si celles-ci sont requises au titre de l'article 26;

(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.

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

Article 33

Principes généraux applicables aux transferts de données à caractère personnel

Les États membres prévoient qu'un transfert, par des autorités compétentes, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après leur transfert

vers un pays tiers ou à une organisation internationale, y compris un transfert ultérieur vers un autre pays tiers ou une autre organisation internationale, ne peut avoir lieu que si:

a) le transfert est nécessaire 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

b) les conditions énoncées dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant.

Article 34

Transferts assortis d'une décision constatant le caractère adéquat du niveau de protection

1. Les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers ou une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision, conformément à l'article 41 du règlement (UE) …./2012 ou conformément au paragraphe 3 du présent article, 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'il n'existe aucune décision adoptée en vertu de l'article 41 du règlement (UE) …./2012, la Commission apprécie le caractère adéquat du niveau de protection en prenant 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 sûreté de l'État et le droit pénal, 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 la personne concernée dans l'exercice de ses 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, dans les limites de la présente directive, qu'un pays tiers, un territoire ou un secteur de traitement de données dans ce pays tiers, 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 57, 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, dans les limites de la présente directive, qu'un pays tiers, 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 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 57, 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 57, paragraphe 3.

6. Les États membres veillent à ce que, lorsque la Commission adopte une décision en vertu du paragraphe 5, selon laquelle tout transfert de données à caractère personnel vers le pays tiers, un territoire ou un secteur de traitement de données dans ce pays tiers, ou à l'organisation internationale en question est interdit, cette décision soit sans préjudice des transferts effectués au titre de l'article 35, paragraphe 1, ou conformément à l'article 36. 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 du présent article.

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. La Commission contrôle l'application des actes d'exécution visés aux paragraphes 3 et 5.

Article 35
Transferts moyennant des garanties appropriées

1. Lorsque la Commission n'a pas adopté de décision en vertu l'article 34, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers ou une organisation internationale ne peut avoir lieu que si:

   a) des garanties appropriées en ce qui concerne la protection des données à caractère personnel ont été offertes dans un instrument juridiquement contraignant; ou

   b) le responsable du traitement ou le sous-traitant a évalué toutes les circonstances entourant le transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.

1. La décision de transfert au titre du paragraphe 1, point b), doit être prise par un personnel dûment habilité. Tout transfert de ce type doit faire l'objet d'une

documentation, qui doit être mise à la disposition de l'autorité de contrôle, sur demande.

Article 36
Dérogations

Par dérogation aux articles 34 et 35, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si:

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

b) le transfert est nécessaire à la sauvegarde des intérêts légitimes de la personne concernée lorsque la législation de l'État membre transférant les données à caractère personnel le prévoit; ou

c) le transfert de données est essentiel pour prévenir une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers; ou

d) le transfert est nécessaire dans des cas particuliers 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; ou

e) le transfert est nécessaire, dans des cas particuliers, à la constatation, à l'exercice ou à la défense d'un droit en justice en rapport avec la prévention et la détection des infractions pénales, des enquêtes et des poursuites en la matière, ou l'exécution de sanctions pénales;

Article 37
Conditions spécifiques applicables au transfert de données à caractère personnel

Les États membres prévoient que le responsable du traitement informe le destinataire des données à caractère personnel de toute limitation du traitement et qu'il prend toutes les mesures raisonnables afin de garantir que ces limitations soient respectées.

Article 38
Coopération internationale dans le domaine de la protection des données à caractère personnel

1. La Commission et les États membres 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 pour 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 34, paragraphe 3.

CHAPITRE VI
AUTORITÉS DE CONTRÔLE INDÉPENDANTES

SECTION 1
STATUT D'INDÉPENDANCE

Article 39
Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application des dispositions adoptées conformément à la présente directive 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. Les États membres peuvent prévoir que l'autorité de contrôle qu'ils instituent conformément au règlement (UE) n° …/2012 prend en charge les fonctions de l'autorité de contrôle devant être instituée conformément au paragraphe 1 du présent article.

3. 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.

Article 40
Indépendance

1. Les États membres veillent à ce que l'autorité de contrôle exerce en toute indépendance les missions et les pouvoirs qui lui sont confiés.

2. Chaque État membre prévoit que les membres de l'autorité de contrôle, dans l'accomplissement de leur mission, 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 obligatoirement 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 41
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.

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 42
Règles relatives à l'établissement de l'autorité de contrôle

Chaque État membre prévoit par voie législative:

a) l'établissement et le statut d'indépendance de l'autorité de contrôle conformément aux articles 39 et 40;

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 de la présente directive, qui peut être d'une durée plus courte;

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 43
Secret professionnel

Les États membres prévoient que 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 44
Compétence

1. Les États membres prévoient que chaque autorité de contrôle exerce, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément à la présente directive.

2. Les États membres prévoient que l'autorité de contrôle n'est pas compétente pour contrôler les traitements effectués par les juridictions dans l'exercice de leurs fonctions juridictionnelles.

Article 45
Fonctions

1. Les États membres prévoient que l'autorité de contrôle:

   (a) contrôle et assure l'application des dispositions adoptées conformément à la présente directive et de ses mesures d'exécution;

   (b) reçoit les réclamations introduites par toute personne concernée ou par une association la représentant et dûment mandatée par elle conformément à l'article 50, 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 lorsqu'un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire;

   (c) vérifie la licéité du traitement de données en vertu de l'article 14, et informe la personne concernée dans un délai raisonnable de l'issue de la vérification ou des motifs ayant empêché sa réalisation;

   (d) fournit une assistance mutuelle à d'autres autorités de contrôle et veille à la cohérence de l’application des dispositions adoptées conformément à la présente directive et des mesures prises pour en assurer le respect;

   (e) 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 a saisi l'autorité de contrôle d'une réclamation, du résultat de ses enquêtes dans un délai raisonnable;

   (f) 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;

(g) 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;

(h) est consultée sur les traitements conformément à l'article 26;

(i) 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 de la présente directive 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. Les États membres prévoient que l'accomplissement des fonctions de l'autorité de contrôle est gratuit pour la personne concernée.

6. Lorsque les demandes sont abusives, 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 abusif de la demande.

Article 46
Pouvoirs

Les États membres prévoient que chaque autorité de contrôle doit notamment être dotée des pouvoirs suivants:

a) des pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle;

b) de pouvoirs effectifs d'intervention, tels que celui de rendre des avis préalablement à la mise en œuvre des traitements et d'assurer une publication appropriée de ces avis, d'ordonner la limitation, l'effacement ou la destruction de données, d'interdire temporairement ou définitivement un traitement, d'adresser un avertissement ou une admonestation au responsable du traitement ou de saisir les parlements nationaux ou d'autres institutions politiques;

c) le pouvoir d'ester en justice en cas de violation des dispositions nationales adoptées en application de la présente directive ou le pouvoir de porter cette violation à la connaissance de l'autorité judiciaire.

Article 47
Rapport d'activité

Les États membres prévoient que chaque autorité de contrôle établit un rapport annuel sur son activité. Le rapport est mis à la disposition de la Commission et du comité européen de la protection des données.

CHAPITRE VII
COOPÉRATION

Article 48
Assistance mutuelle

1. Les États membres prévoient que les autorités de contrôle se prêtent une assistance mutuelle en vue de mettre en œuvre et d'appliquer de manière cohérente les dispositions adoptées conformément à la présente directive, et qu'elles 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 de consultation préalable, d'inspection et d'enquête.

2. Les États membres prévoient qu'une autorité de contrôle prend toutes les mesures appropriées requises pour répondre à la demande d'une autre autorité de contrôle.

3. 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.

Article 49
Missions du comité européen de la protection des données

1. Le comité européen de la protection des données institué par le règlement (EU) …./2012 accomplit les missions suivantes en ce qui concerne les activités de traitement relevant du champ d'application de la présente directive:

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

   (b) examiner, à la demande de la Commission, de sa propre initiative ou à l'initiative de l'un de ses membres, toute question portant sur l'application des dispositions adoptées conformément à la présente directive, et publier des lignes directrices, des recommandations et des bonnes pratiques adressées aux autorités de contrôle, afin de favoriser l'application cohérente desdites dispositions;

   (c) faire le bilan de l'application pratique des lignes directrices, recommandations et bonnes pratiques visées au point b) et faire régulièrement rapport à la Commission sur ces mesures;

(d) communiquer à la Commission un avis sur le niveau de protection assuré dans des pays tiers ou des organisations internationales;

(e) promouvoir la coopération et l'échange bilatéral et multilatéral effectif d'informations et de pratiques entre les autorités de contrôle;

(f) promouvoir l'élaboration de programmes de formation conjoints et 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) promouvoir l'échange, avec des autorités de contrôle de la protection des données de tous pays, de connaissances et de documentation, notamment 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 57, 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.

CHAPITRE VIII
RECOURS, RESPONSABILITÉ ET SANCTIONS

Article 50

Droit d'introduire une réclamation auprès d'une autorité de contrôle

1. Sans préjudice de tout autre recours administratif ou judiciaire, les États membres prévoient que 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 ne respecte pas les dispositions adoptées conformément à la présente directive.

2. Les États membres prévoient que 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 est 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 de la présente droits ont été violés à la suite du traitement de données à caractère personnel. L'organisation ou l'association doivent être dûment mandatées par la ou les personne(s) concernée(s).

3. Les États membres prévoient que tout organisme, organisation ou association visé au paragraphe 2 a le droit, indépendamment d'une réclamation introduite par une

personne concernée, de saisir une autorité de contrôle d'une réclamation dans tout État membre s'il considère qu'il y a eu violation de données à caractère personnel.

Article 51

Droit à un recours juridictionnel contre une autorité de contrôle

1. Les États membres prévoient le droit à un recours juridictionnel contre les décisions d'une autorité de contrôle.

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 45, paragraphe 1, point b).

3. Les États membres prévoient que 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.

Article 52

Droit à un recours juridictionnel contre un responsable du traitement ou un sous-traitant

Les États membres prévoient que, sans préjudice de tout recours administratif qui lui est ouvert, notamment le droit 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 la présente directive, à la suite du traitement de données à caractère personnel la concernant, effectué en violation des dispositions de ladite directive.

Article 53

Règles communes pour les procédures juridictionnelles

1. Les États membres prévoient que tout organisme, organisation ou association visé à l'article 50, paragraphe 2, est habilité à exercer les droits prévus aux articles 51 et 52 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 adoptées conformément à la présente directive ou d'assurer la cohérence de la protection des données à caractère personnel au sein de l'Union.

3. 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 54
Responsabilité et droit à réparation

1. Les États membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions adoptées conformément à la présente directive 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 55
Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions adoptées conformément à la présente directive et prennent toute mesure nécessaire pour garantir leur application. Les sanctions ainsi prévues doivent être effectives, proportionnées et dissuasives.

CHAPITRE IX
ACTES DÉLÉGUÉS ET ACTES D'EXÉCUTION

Article 56
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 28, paragraphe 5, est conférée à la Commission pour une durée indéterminée à compter de la date d’entrée en vigueur de la présente directive.

3. La délégation de pouvoir visée à l'article 28, paragraphe 5, 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 28, paragraphe 5, 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 57
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 X
DISPOSITIONS FINALES

Article 58
Abrogation

1. La décision-cadre 2008/977/JAI du Conseil est abrogée.

2. Les références faites à la décision-cadre abrogée visée au paragraphe 1 s'entendent comme faites à la présente directive.

Article 59
Relation avec les actes de l'Union adoptés antérieurement dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière

Les dispositions spécifiques à la protection des données à caractère personnel à l'égard du traitement de ces données 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, figurant dans des actes de l'Union adoptés avant la date d'adoption de la présente directive qui régissent le traitement des données à caractère personnel entre États membres et l'accès des autorités nationales désignées aux systèmes d'information créés en vertu des traités, dans le cadre de la présente directive, demeurent inchangées.

Article 60
Relation avec les accords internationaux conclus antérieurement dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière

Les accords internationaux conclus par les États membres avant l'entrée en vigueur de la présente directive sont modifiés, en tant que de besoin, dans un délai de cinq ans à compter de son entrée en vigueur.

Article 61
Évaluation

1. La Commission évalue l'application de la présente directive.

2. Dans un délai de trois ans à compter de l'entrée en vigueur de la présente directive, la Commission réexamine d'autres actes adoptés par l'Union européenne qui régissent le 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, notamment les actes adoptés par l'Union qui sont mentionnés à l'article 59, afin d'apprécier la nécessité de les mettre en conformité avec la présente directive et de formuler, le cas échéant, les propositions nécessaires en vue de modifier ces actes pour assurer une approche cohérente de la protection des données à caractère personnel dans le cadre de la présente directive.

3. La Commission présente périodiquement des rapports sur l'évaluation et la révision de la présente directive au Parlement européen et au Conseil, conformément au paragraphe 1. Le premier rapport est présenté au plus tard quatre ans après l'entrée en vigueur de la présente directive. Les rapports suivants sont ensuite présentés tous les quatre ans. La Commission soumet, si nécessaire, les propositions ad hoc pour modifier la présente directive et harmoniser d'autres instruments juridiques. Le rapport est publié.

Article 62
Transposition

1. Les États membres adoptent et publient, au plus tard le [date/deux ans après l'entrée en vigueur], les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils notifient immédiatement à la Commission le texte de ces dispositions.

   Ils appliquent lesdites dispositions à compter du xx.xx.201x [date/deux ans après l'entrée en vigueur].

   Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des principales dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 63
Entrée en vigueur et application

La présente directive entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 64
Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le 25.1.2012

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