III

(Actes pris en application du traité UE)

ACTES PRIS EN APPLICATION DU TITRE VI DU TRAITÉ UE

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

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment ses articles 30 et 31 et son article 34, paragraphe 2, point b),

vu la proposition de la Commission,

vu l'avis du Parlement européen [1],

considérant ce qui suit:

(1) L'Union européenne s'est fixé pour objectif de maintenir et de développer un espace de liberté, de sécurité et de justice dans lequel un niveau élevé de protection doit être assuré par le biais d'une action en commun des États membres dans le domaine de la coopération policière et judiciaire en matière pénale.

(2) L'action en commun dans le domaine de la coopération policière aux termes de l'article 30, paragraphe 1, point b), du traité sur l'Union européenne et l'action en commun dans le domaine de la coopération judiciaire en matière pénale aux termes de l'article 31, paragraphe 1, point a), du traité sur l'Union européenne supposent le traitement des informations pertinentes qui devraient faire l'objet de dispositions appropriées relatives à la protection des données à caractère personnel.

(3) La législation qui relève du titre VI du traité sur l'Union européenne devrait promouvoir la coopération policière et judiciaire en matière pénale du point de vue de son efficacité, de sa légitimité et du respect des droits fondamentaux, en particulier du droit au respect de la vie privée et du droit à la protection des données à caractère personnel. Des normes communes relatives au traitement et à la protection des données à caractère personnel traitées dans le but de prévenir et de combattre la criminalité contribuent à la réalisation de ces deux objectifs.

(4) Le programme de La Haye visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne, adopté par le Conseil européen le 4 novembre 2004, a souligné la nécessité d'une approche innovante de l'échange transfrontière d'informations en matière répressive, dans le strict respect de certaines conditions fondamentales dans le domaine de la protection des données, et a invité la Commission à présenter des propositions à cet égard avant la fin de 2005 au plus tard. C'est ce que reflète le plan d'action du Conseil et de la Commission mettant en œuvre le programme de La Haye visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne [2].

(5) L'échange de données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale, et notamment de la mise en œuvre du principe de disponibilité des informations au sens du programme de La Haye, devrait être étayé par des règles claires qui renforcent la confiance mutuelle entre les autorités compétentes et garantissent la protection des informations pertinentes en excluant toute discrimination concernant cette coopération entre les États membres tout en respectant pleinement les droits fondamentaux des personnes. Les instruments qui existent au niveau européen ne sont pas suffisants. 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 [3] ne s'applique pas au traitement des données à caractère personnel dans le cadre d'une activité qui n'entre pas dans le champ d'application du droit communautaire, comme les activités prévues par le titre VI du traité sur l'Union européenne, et en tout cas pas aux opérations de traitement concernant la sécurité publique, la défense, la sécurité de l'État ou les activités de l'État en matière pénale.

[1] JO C 125 E du 22.5.2008, p. 154.

[2] JO C 198 du 12.8.2005, p. 1.

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

(6) La présente décision-cadre ne s'applique qu'aux données collectées ou traitées 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. La décision-cadre devrait laisser aux États membres le soin de déterminer plus précisément au niveau national quelles autres fins doivent être considérées comme incompatibles avec l'objectif pour lequel les données à caractère personnel sont collectées à l'origine. En général, le traitement ultérieur à des fins historiques, statistiques ou scientifiques ne devrait pas être considéré comme incompatible avec l'objectif initial du traitement.

(7) Le champ d'application de la décision-cadre est limité au traitement des données à caractère personnel transmises ou mises à disposition entre les États membres. Aucune conclusion ne devrait pouvoir être tirée de cette limitation quant à la compétence de l'Union pour adopter des actes relatifs à la collecte et au traitement de données à caractère personnel au niveau national ou à l'opportunité pour l'Union d'agir en ce sens à l'avenir.

(8) Pour faciliter les échanges de données dans l'Union, les États membres se proposent de faire en sorte que le niveau de protection des données atteint pour le traitement de données à l'échelon national corresponde à celui prévu par la présente décision-cadre. En ce qui concerne le traitement national des données, la présente décision-cadre n'empêche pas les États membres de prévoir pour la protection des données à caractère personnel des garanties plus rigoureuses que celles qui sont établies par la présente décision-cadre.

(9) La présente décision-cadre ne devrait pas s'appliquer aux données à caractère personnel qu'un État membre a obtenues en application de la présente décision-cadre et qui proviennent de cet État membre.

(10) Le rapprochement des législations des États membres ne devrait pas entraîner un affaiblissement de la protection des données qu'elles assurent mais devrait, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans l'Union.

(11) Il convient de préciser les objectifs en matière de protection des données dans le cadre des activités policières et judiciaires et de définir les règles concernant la licéité du traitement des données à caractère personnel, afin de garantir que toute information susceptible d'être échangée soit traitée en toute licéité et dans le respect des principes fondamentaux relatifs à la qualité des données. En même temps, les activités légitimes de la police, des douanes, des autorités judiciaires et autres autorités compétentes ne sauraient être compromises.

(12) Il convient d'appliquer le principe d'exactitude des données en tenant compte de la nature et de l'objet du traitement concerné. Par exemple, en particulier au cours d'une procédure judiciaire, les données sont fondées sur des perceptions personnelles subjectives et ne sont pas du tout vérifiables dans certains cas. L'exigence en matière d'exactitude ne peut donc pas s'appliquer à l'exactitude d'une déclaration mais simplement au fait qu'une déclaration spécifique a été faite.

(13) L'archivage dans un ensemble de données distinct devrait être autorisé si les données ne sont plus nécessaires et utilisées pour la prévention et la détection des infractions pénales, ainsi que pour les enquêtes et les poursuites en la matière ou l'exécution des sanctions pénales. L'archivage dans un ensemble de données distinct devrait également être autorisé si les données archivées sont conservées dans une base de données avec d'autres données d'une telle manière qu'elles ne peuvent plus être utilisées pour la prévention et la détection des infractions pénales, ainsi que pour les enquêtes et les poursuites en la matière ou l'exécution des sanctions pénales. La pertinence de la durée d'archivage devrait dépendre des fins de l'archivage et des intérêts légitimes des personnes concernées. Dans le cas d'un archivage à des fins historiques, une période très longue peut aussi être envisagée.

(14) On peut également effacer les données en détruisant leur support.

(15) En ce qui concerne les données inexactes, incomplètes ou périmées qui sont transmises à un autre État membre ou mises à sa disposition et traitées ultérieurement par des autorités quasi judiciaires, c'est-à-dire des autorités compétentes pour prendre des décisions juridiquement contraignantes, leur rectification, effacement ou verrouillage devrait être effectué conformément au droit national.

(16) Pour garantir un niveau élevé de protection des données à caractère personnel des personnes, des dispositions communes permettant de déterminer la légalité et la qualité des données traitées par les autorités compétentes des autres États membres sont nécessaires.

(17) Il est opportun de définir au niveau européen les conditions dans lesquelles les autorités compétentes des États membres devraient être autorisées à transmettre des données à caractère personnel reçues d'autres États membres à des autorités et des personnes privées dans les États membres et à les mettre à leur disposition. Dans bon nombre de cas, les services judiciaires, de police ou douaniers doivent transmettre des données à caractère personnel à des personnes privées pour poursuivre des crimes ou prévenir un danger immédiat et sérieux pour la sécurité publique ou une atteinte grave aux droits des personnes, par exemple en signalant de faux titres aux banques et établissements de crédit, ou dans le domaine de la criminalité visant les véhicules, en communiquant des données à caractère personnel aux sociétés d'assurances afin d'empêcher le trafic de véhicules à moteur volés ou d'améliorer les conditions de récupération à l'étranger des véhicules à moteur volés. Cela n'implique pas le transfert de missions de police ou de justice à des personnes privées.

(18) Les règles de la présente décision-cadre relatives à la transmission à des personnes privées de données à caractère personnel par les services judiciaires, de police ou douaniers ne s'appliquent pas à la transmission de données à des personnes privées (telles que les avocats de la défense et les victimes) dans le cadre de la procédure pénale.

(19) Le traitement ultérieur des données à caractère personnel transmises ou mises à disposition par l'autorité compétente d'un autre État membre, en particulier la transmission ou la mise à disposition ultérieures de ces données, devrait être régi par des règles communes au niveau européen.

(20) Lorsque des données à caractère personnel peuvent faire l'objet d'un traitement ultérieur après que l'État membre auprès duquel les données ont été collectées a donné son accord au transfert, chaque État membre devrait être en mesure de déterminer les modalités d'un tel accord, y compris, par exemple, par le biais d'un accord général pour des catégories d'informations ou des catégories de traitement ultérieur.

(21) Lorsque des données à caractère personnel peuvent faire l'objet d'un traitement ultérieur aux fins de procédures administratives, ces dernières incluent aussi les activités menées par des autorités de réglementation et de contrôle.

(22) Les activités légitimes de la police, des douanes, des autorités judiciaires et autres autorités compétentes peuvent nécessiter la transmission de données à des autorités d'États tiers ou à des instances internationales qui ont des obligations en matière de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales.

(23) Lorsque des données à caractère personnel sont transférées d'un État membre vers des États tiers ou des instances internationales, ces données devraient, par principe, bénéficier d'un niveau de protection suffisant.

(24) Lorsque des données à caractère personnel sont transférées d'un État membre vers des États tiers ou des instances internationales, un tel transfert ne devrait en principe avoir lieu qu'après que l'État membre auprès duquel les données ont été collectées a donné son accord au transfert. Chaque État membre devrait être en mesure de déterminer les modalités d'un tel accord, y compris, par exemple, par le biais d'un accord général pour des catégories d'informations ou des États tiers spécifiques.

(25) Il est dans l'intérêt d'une coopération efficace en matière répressive que, lorsque le caractère immédiat de la menace pour la sécurité publique d'un État membre ou d'un État tiers est tel qu'il rend impossible l'obtention d'un accord préalable en temps utile, l'autorité compétente soit en mesure de transférer les données à caractère personnel pertinentes à l'État tiers concerné sans un tel accord préalable. Il pourrait en être de même lorsque d'autres intérêts essentiels d'un État membre d'importance égale sont en jeu, par exemple, lorsque l'infrastructure critique d'un État membre pourrait faire l'objet d'une menace immédiate et grave ou lorsque le système financier d'un État membre pourrait être sérieusement perturbé.

(26) Il peut être impératif d'informer la personne concernée du traitement de ses données, en particulier dans le cas d'atteintes particulièrement graves à ses droits à la suite de mesures relatives à la collecte de données secrètes, afin de lui garantir une protection juridique effective.

(27) Les États membres devraient veiller à ce que la personne concernée soit informée que ses données à caractère personnel pourraient être ou sont collectées, traitées ou transmises à un autre État membre 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. Les modalités du droit de la personne concernée d'être informée et les exceptions en la matière devraient être déterminées par la législation nationale. Cela peut se faire sous une forme générale, par exemple au moyen d'un acte législatif ou par la publication d'une liste des traitements.

(28) Pour garantir la protection des données à caractère personnel sans compromettre la finalité d'une enquête pénale, il est nécessaire de définir les droits de la personne concernée.

(29) Certains États membres ont assuré le droit d'accès de la personne concernée en matière pénale par le biais d'un système dans le cadre duquel l'autorité de contrôle nationale a accès, à la place de la personne concernée, à toutes les données à caractère personnel relatives à cette dernière sans aucune restriction, et peut également rectifier, effacer ou mettre à jour les données inexactes. Dans un tel cas d'accès indirect, le droit national de ces États membres peut prévoir que l'autorité de contrôle nationale informera seulement la personne concernée que toutes les vérifications nécessaires ont été effectuées. Toutefois, ces États membres prévoient également des possibilités d'accès direct pour la personne concernée dans des cas spécifiques, comme un accès à des dossiers judiciaires, ou bien pour obtenir des copies de leur dossier pénal ou de documents relatifs à leurs auditions par les services de police.

(30) Il est opportun de fixer des règles communes en matière de confidentialité et de sécurité du traitement, de responsabilité et de sanctions en cas d'utilisation illicite par les autorités compétentes, ainsi que de voies de recours offertes à la personne concernée. Il appartient néanmoins à chaque État membre de déterminer la nature des règles en matière de responsabilité délictuelle et des sanctions applicables en cas de violation des dispositions nationales sur la protection des données.

(31) La présente décision-cadre permet de tenir compte du principe d'accès du public aux documents officiels lors de la mise en œuvre des principes qu'elle énonce.

(32) Lorsqu'il est nécessaire de protéger des données à caractère personnel en ce qui concerne un traitement qui, par son ampleur ou son type, présente des risques spécifiques pour les libertés et les droits fondamentaux, par exemple un traitement au moyen de nouveaux mécanismes, technologies ou procédures, il convient de faire en sorte que les autorités de contrôle nationales compétentes soient consultées avant l'établissement des fichiers destinés au traitement de ces données.

(33) La création, dans les États membres, d'autorités de contrôle exerçant leurs fonctions en toute indépendance est une composante essentielle de la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire entre les États membres.

(34) Les autorités de contrôle déjà mises en place dans les États membres en vertu de la directive 95/46/CE peuvent aussi prendre en charge les tâches qui doivent être accomplies par les autorités de contrôle nationales mises en place conformément à la présente décision-cadre.

(35) Ces autorités de contôle devraient être dotées des moyens nécessaires à l'exécution de leurs tâches, qu'il s'agisse des pouvoirs d'investigation et d'intervention, en particulier lorsqu'elles sont saisies de réclamations émanant de particuliers, ou du pouvoir d'ester en justice. Ces autorités de contôle devraient contribuer à garantir la transparence du traitement de données effectué dans les États membres dont elles relèvent. Toutefois, leurs pouvoirs ne devraient interférer ni avec les règles spécifiques fixées pour la procédure pénale, ni avec l'indépendance du pouvoir judiciaire.

(36) Aux termes de l'article 47 du traité sur l'Union européenne, rien dans ledit traité ne doit affecter les traités instituant les Communautés européennes ni les traités et actes subséquents qui les ont modifiés ou complétés. En conséquence, la présente décision-cadre n'affecte pas la protection des données à caractère personnel régie par le droit communautaire, notamment telle que prévue par la directive 95/46/CE, le 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 [1], ainsi que la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») [2].

(37) La présente décision-cadre est sans préjudice des règles sur l'accès illicite aux données prévues par la décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information [3].

(38) La présente décision-cadre est sans préjudice des obligations et engagements existants incombant aux États membres ou à l'Union en vertu des accords bilatéraux et/ou multilatéraux avec des États tiers. Il convient que les futurs accords respectent les règles relatives aux échanges avec des États tiers.

(39) Plusieurs actes, adoptés sur la base du titre VI du traité sur l'Union européenne, comportent des dispositions spécifiques relatives à la protection des données à caractère personnel échangées ou traitées en vertu de ces actes. Dans certains cas, ces dispositions constituent un ensemble complet et cohérent de règles couvrant tous les aspects pertinents de la protection des données (principes de qualité des données, règles relatives à la sécurité des données, réglementation des droits des personnes concernées et des garanties qui leur sont offertes, organisation du contrôle et responsabilité) et régissent ces matières de manière plus détaillée que ne le fait la présente décision-cadre. L'ensemble correspondant des dispositions relatives à la protection des données figurant dans ces actes, en particulier celles qui régissent le fonctionnement d'Europol, d'Eurojust, du système d'information Schengen (SIS) et du système d'information douanier (SID), ainsi que celles qui prévoient l'accès direct des autorités des États membres à certains systèmes de données d'autres États membres, ne devrait pas être affecté par la présente décision-cadre. Il en va de même des dispositions relatives à la protection des données qui régissent le transfert automatisé entre États membres de profils ADN, de données dactyloscopiques et de données nationales relatives à l'immatriculation des véhicules au titre de la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière [4].

(40) Dans d'autres cas, les dispositions relatives à la protection des données figurant dans des actes adoptés sur la base du titre VI du traité sur l'Union européenne ont un champ d'application plus limité. Elles prévoient souvent, pour les États membres qui reçoivent des informations contenant des données à caractère personnel d'autres États membres, des conditions spécifiques en ce qui concerne les fins pour lesquelles ils peuvent utiliser ces données, mais elles renvoient, pour d'autres aspects de la protection des données, à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ou au droit national. Dans la mesure où les dispositions qui figurent dans ces actes imposent aux États membres destinataires, en ce qui concerne l'utilisation ou le transfert ultérieur de données à caractère personnel, des conditions plus restrictives que celles figurant dans les dispositions correspondantes de la présente décision-cadre, les premières citées ne devraient pas s'en trouver affectées. Cependant, pour tous les autres aspects, les règles prévues dans la présente décision-cadre devraient s'appliquer.

(41) La présente décision-cadre n'a pas d'incidence sur la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, le protocole additionnel à cette convention du 8 novembre 2001 ou les conventions du Conseil de l'Europe sur la coopération judiciaire en matière pénale.

[1] JO L 8 du 12.1.2001, p. 1.
[2] JO L 201 du 31.7.2002, p. 37.
[3] JO L 69 du 16.3.2005, p. 67.
[4] JO L 210 du 6.8.2008, p. 1.

(42) Étant donné que les objectifs de la présente décision-cadre, à savoir définir des règles communes pour la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, ne peuvent pas être réalisés de manière suffisante par les États membres, et peuvent donc en raison des dimensions et des effets de l'action envisagée être mieux réalisés au niveau de l'Union, l'Union peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité instituant la Communauté européenne et visé à l'article 2 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé à l'article 5 du traité instituant la Communauté européenne, la présente décision-cadre n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(43) Le Royaume-Uni participe à la présente décision-cadre conformément à l'article 5 du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne annexé au traité sur l'Union européenne et au traité instituant la Communauté européenne et à l'article 8, paragraphe 2, de la décision 2000/365/CE du Conseil du 29 mai 2000 relative à la demande du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de participer à certaines dispositions de l'acquis de Schengen [1].

(44) L'Irlande participe à la présente décision-cadre conformément à l'article 5 du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne annexé au traité sur l'Union européenne et au traité instituant la Communauté européenne et à l'article 6, paragraphe 2, de la décision 2002/192/CE du Conseil du 28 février 2002 relative à la demande de l'Irlande de participer à certaines dispositions de l'acquis de Schengen [2].

(45) En ce qui concerne l'Islande et la Norvège, la présente décision-cadre constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne et la République d'Islande et le Royaume de Norvège sur l'association de ces États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen [3], qui relève du domaine visé à l'article 1er, points H et I, de la décision 1999/437/CE du Conseil [4] relative à certaines modalités d'application dudit accord.

(46) En ce qui concerne la Suisse, la présente décision-cadre constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu 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 [5], qui relève du domaine visé à l'article 1er, points H et I, de la décision 1999/437/CE en liaison avec l'article 3 de la décision 2008/149/JAI du Conseil [6] relative à la conclusion, au nom de l'Union européenne, dudit accord.

(47) En ce qui concerne le Liechtenstein, la présente décision-cadre 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, qui relève du domaine visé à l'article 1er, points H et I, de la décision 1999/437/CE en liaison avec l'article 3 de la décision 2008/262/JAI du Conseil [7] relative à la signature, au nom de l'Union européenne, dudit protocole.

(48) La présente décision-cadre respecte les droits fondamentaux et observe les principes reconnus, en particulier, par la charte des droits fondamentaux de l'Union européenne [8]. Elle tend à préserver pleinement le droit au respect de la vie privée et le droit à la protection des données à caractère personnel consacrés aux articles 7 et 8 de la charte,

A ARRÊTÉ LA PRÉSENTE DÉCISION:

Article premier

Objet et champ d'application

1. La présente décision-cadre a pour but de garantir à la fois un niveau élevé de protection des droits et libertés fondamentaux des personnes physiques, en particulier leur droit au respect de la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale prévue par le titre VI du traité sur l'Union européenne et un niveau élevé de sécurité publique.

2. Conformément à la présente décision-cadre, les États membres protègent les droits et libertés fondamentaux des personnes physiques, en particulier leur droit au respect de la vie privée, lorsque, 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, des données à caractère personnel:

a) sont ou ont été transmises ou mises à disposition entre les États membres,

[1] JO L 131 du 1.6.2000, p. 43.
[2] JO L 64 du 7.3.2002, p. 20.
[3] JO L 176 du 10.7.1999, p. 36.
[4] JO L 176 du 10.7.1999, p. 31.
[5] JO L 53 du 27.2.2008, p. 52.
[6] JO L 53 du 27.2.2008, p. 50.
[7] JO L 83 du 26.3.2008, p. 5.
[8] JO C 303 du 14.12.2007, p. 1.

b) sont ou ont été transmises à des autorités ou des systèmes d'information créés sur la base du titre VI du traité sur l'Union européenne ou mises à leur disposition par des États membres, ou

c) sont ou ont été transmises aux autorités compétentes des États membres, ou mises à leur disposition, par des autorités ou des systèmes d'information créés sur la base du traité sur l'Union européenne ou du traité instituant la Communauté européenne.

3. La présente décision-cadre 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.

4. La présente décision-cadre est sans préjudice des intérêts essentiels en matière de sécurité nationale et des activités de renseignement spécifiques dans le domaine de la sécurité nationale.

5. La présente décision-cadre n'empêche pas les États membres de prévoir, pour la protection des données à caractère personnel collectées ou traitées au niveau national, des garanties plus rigoureuses que celles établies par la présente décision-cadre.

Article 2

Définitions

Aux fins de la présente décision-cadre, on entend par:

a) «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;

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

c) «verrouillage»: le marquage de données à caractère personnel enregistrées, en vue de limiter leur traitement futur;

d) «fichier de données à caractère personnel» et «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;

e) «sous-traitant»: tout organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

f) «destinataire»: tout organisme qui reçoit communication de données;

g) «consentement de la personne concernée»: toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement;

h) «autorités compétentes»: les agences ou organismes créés en vertu d'actes juridiques adoptés par le Conseil en vertu du titre VI du traité sur l'Union européenne, ainsi que les autorités de police, les autorités douanières, les autorités judiciaires et les autres autorités compétentes des États membres qui sont autorisées par le droit national à traiter des données à caractère personnel dans le cadre du champ d'application de la présente décision-cadre;

i) «responsable du traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel;

j) «marquage»: l'apposition d'une marque sur des données à caractère personnel enregistrées sans chercher à limiter leur traitement futur;

k) «rendre anonyme»: le fait de modifier des données à caractère personnel d'une façon telle que des données particulières sur des situations personnelles ou matérielles ne puissent plus être rattachées à une personne physique identifiée ou identifiable ou alors seulement moyennant un effort démesuré en termes de temps, de coût et de main-d'œuvre.

Article 3

Principes de licéité, de proportionnalité et de finalité

1. Les données à caractère personnel peuvent être collectées par les autorités compétentes uniquement pour des finalités déterminées, explicites et licites dans le cadre de leurs tâches et traitées uniquement pour les finalités pour lesquelles elles ont été collectées. Le traitement des données est licite et adéquat, pertinent et non excessif au regard des finalités pour lesquelles elles sont collectées.

2. Le traitement ultérieur des données pour une autre finalité est permis, dans la mesure où:

a) ce traitement n'est pas incompatible avec la finalité pour laquelle les données ont été collectées;

b) les autorités compétentes sont autorisées à traiter ces données pour d'autres finalités conformément aux dispositions légales applicables; et

c) ce traitement est nécessaire et proportionné à ces finalités.

En outre, les données à caractère personnel transmises peuvent être traitées ultérieurement par les autorités compétentes à des fins historiques, statistiques ou scientifiques, dans la mesure où les États membres prévoient des garanties appropriées, comme le fait de rendre les données anonymes.

Article 4

Rectification, effacement et verrouillage

1. Les données à caractère personnel sont rectifiées lorsqu'elles sont inexactes et, si possible et si nécessaire, complétées ou actualisées.

2. Les données à caractère personnel sont effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires pour les finalités pour lesquelles elles ont licitement été collectées ou sont licitement traitées ultérieurement. L'archivage de ces données dans un ensemble de données distinct pendant une période appropriée conformément à la législation nationale n'est pas concerné par la présente disposition.

3. Les données à caractère personnel ne sont pas effacées, mais seulement verrouillées lorsqu'il y a de bonnes raisons de croire que leur effacement pourrait porter atteinte aux intérêts légitimes de la personne concernée. Les données verrouillées ne sont traitées que pour les finalités qui ont empêché leur effacement.

4. Lorsque les données à caractère personnel figurent dans une décision de justice ou un dossier judiciaire lié à l'adoption d'une décision de justice, la rectification, l'effacement ou le verrouillage est effectué conformément aux règles nationales sur les procédures judiciaires.

Article 5

Fixation de délais d'effacement et de vérification

Des délais appropriés sont prévus pour effacer les données à caractère personnel ou vérifier régulièrement s'il est nécessaire de conserver les données. Des règles procédurales permettent d'assurer le respect de ces délais.

Article 6

Traitements portant sur des catégories particulières de données

Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle n'est autorisé que par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

Article 7

Décisions individuelles automatisées

Une décision qui produits des effets juridiques défavorables pour la personne concernée ou qui l'affecte de manière significative et qui est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité n'est autorisée que si la sauvegarde des intérêts légitimes de la personne concernée est assurée par la loi.

Article 8

Vérification de la qualité des données transmises ou mises à disposition

1. Les autorités compétentes prennent toutes les mesures raisonnables pour faire en sorte que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour ne soient pas transmises ou mises à disposition. À cette fin, les autorités compétentes vérifient, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition. Dans la mesure du possible, lors de toute transmission de données, les informations disponibles sont jointes aux données, afin que l'État membre destinataire puisse juger de l'exactitude, de l'exhaustivité, de l'actualité et de la fiabilité desdites données. Si des données à caractère personnel ont été transmises sans demande préalable, l'autorité destinataire vérifie sans tarder si ces données sont nécessaires à la finalité pour laquelle elles ont été transmises.

2. S'il s'avère que des données inexactes ont été transmises ou que des données ont été transmises illicitement, le destinataire en est informé immédiatement. Les données doivent être rectifiées, effacées ou verrouillées sans délai conformément à l'article 4.

Article 9

Délais

1. L'autorité qui transmet les données peut, au moment de la transmission ou de la mise à disposition des données, dans le cadre du droit national et conformément aux articles 4 et 5, indiquer les délais de conservation des données, le destinataire étant lui aussi tenu d'effacer ou de verrouiller les données ou de vérifier si elles sont ou non encore nécessaires lorsque ces délais sont écoulés. Cette obligation ne s'applique pas si, à l'expiration de ces délais, les données sont nécessaires pour une enquête en cours, la poursuite d'infractions pénales ou l'exécution de sanctions pénales.

2. Lorsque l'autorité qui transmet les données s'est abstenue d'indiquer un délai conformément au paragraphe 1, les délais prévus par le droit national des États membres destinataires, conformément aux articles 4 et 5, pour la conservation des données s'appliquent.

Article 10

Journalisation et documentation

1. Toute transmission de données à caractère personnel est journalisée ou fait l'objet d'une trace documentaire 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.

2. Les journaux ou la documentation élaborés en vertu du paragraphe 1 sont transmis à l'autorité de contrôle compétente pour la protection des données à la demande de cette dernière, aux fins du contrôle de la protection des données. L'autorité de contrôle compétente n'utilise ces informations que pour contrôler la protection des données et garantir le traitement approprié des données ainsi que leur intégrité et leur sécurité.

Article 11

Traitement des données à caractère personnel transmises ou mises à disposition par un autre État membre

Les données à caractère personnel qui ont été transmises ou mises à disposition par l'autorité compétente d'un autre État membre peuvent, conformément aux exigences de l'article 3, paragraphe 2, être traitées ultérieurement pour des finalités autres que celles pour lesquelles elles ont été transmises ou mises à disposition uniquement dans les cas suivants:

a) pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière, ou l'exécution de sanctions pénales, à condition que ces infractions et sanctions soient distinctes de celles pour lesquelles les données ont été transmises ou mises à disposition;

b) pour d'autres procédures judiciaires et administratives directement liées à la prévention et la détection des infractions pénales, aux enquêtes et poursuites en la matière, ou à l'exécution de sanctions pénales;

c) pour prévenir un danger immédiat et sérieux pour la sécurité publique; ou

d) pour toute autre finalité, uniquement avec l'accord préalable de l'État membre qui transmet les données ou avec le consentement de la personne concernée, donné conformément au droit national.

En outre, les données à caractère personnel transmises peuvent être traitées ultérieurement par les autorités compétentes à des fins historiques, statistiques ou scientifiques, dans la mesure où les États membres prévoient des garanties appropriées, comme le fait de rendre les données anonymes.

Article 12

Respect des restrictions de traitement nationales

1. Lorsque, en vertu du droit de l'État membre qui transmet les données, des restrictions de traitement spécifiques s'appliquent dans des circonstances précises à l'échange de données entre les autorités compétentes au sein de cet État membre, l'autorité qui transmet les données informe le destinataire de telles restrictions. Le destinataire veille à ce que ces restrictions de traitement soient respectées.

2. Lorsqu'ils appliquent le paragraphe 1, les États membres n'imposent pas de restrictions concernant les transmissions de données à d'autres États membres ou à des agences ou organismes créés en vertu du titre VI du traité sur l'Union européenne autres que celles applicables aux transmissions nationales de données similaires.

Article 13

Transfert aux autorités compétentes d'États tiers ou à des instances internationales

1. Les États membres font en sorte que les données à caractère personnel qui sont transmises ou mises à disposition par l'autorité compétente d'un autre État membre ne puissent être transférées à des États tiers ou à des instances internationales que si

a) cela 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;

b) l'autorité destinataire de l'État tiers ou l'instance internationale destinataire est chargée de la prévention et de la détection des infractions pénales, des enquêtes et des poursuites en la matière ou de l'exécution des sanctions pénales;

c) l'État membre auprès duquel les données ont été collectées a donné son accord au transfert dans le respect de sa législation nationale, et

d) l'État tiers ou l'instance internationale concerné assure un niveau de protection adéquat pour le traitement de données envisagé.

2. Le transfert sans accord préalable conformément au paragraphe 1, point c), n'est autorisé que si le transfert de données est essentiel pour prévenir un danger immédiat et sérieux pour la sécurité publique d'un État membre ou d'un État tiers ou pour les intérêts essentiels d'un État membre et que l'accord préalable ne peut pas être obtenu en temps utile. L'autorité compétente pour donner cet accord est informée sans délai.

3. Par dérogation au paragraphe 1, point d), les données à caractère personnel peuvent être transférées si

a) la législation nationale de l'État membre qui transfère les données le prévoit

   i) pour des intérêts spécifiques légitimes de la personne concernée, ou

   ii) lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou

b) l'État tiers ou l'instance internationale destinataire prévoit des garanties qui sont jugées adéquates par l'État membre concerné conformément à sa législation nationale.

4. Le caractère adéquat du niveau de protection visé au paragraphe 1, point d), s'apprécie au regard de toutes les circonstances relatives à une opération de transfert ou à un ensemble d'opérations de transfert de données. En particulier, sont pris en considération la nature des données, la finalité et la durée du ou des traitements envisagés, l'État d'origine et l'État ou l'instance internationale de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans l'État tiers ou l'instance internationale en question, ainsi que les règles professionnelles et les mesures de sécurité qui s'y appliquent.

Article 14

Transmission à des personnes privées dans les États membres

1. Les États membres font en sorte que les données à caractère personnel transmises ou mises à disposition par l'autorité compétente d'un autre État membre ne puissent être transmises à des personnes privées que si:

a) l'autorité compétente de l'État membre auprès duquel les données ont été collectées a consenti à la transmission dans le respect de sa législation nationale;

b) aucun intérêt spécifique légitime de la personne concernée n'empêche la transmission, et

c) dans des cas particuliers, le transfert est essentiel pour l'autorité compétente qui transmet les données à une personne privée pour:

i) l'exécution d'une tâche qui lui a été légalement confiée;

ii) la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales;

iii) la prévention d'un danger immédiat et sérieux pour la sécurité publique; ou

iv) la prévention d'une atteinte grave aux droits des personnes.

2. L'autorité compétente qui transmet des données à une personne privée informe cette dernière des fins exclusives auxquelles les données peuvent être utilisées.

Article 15

Informations fournies à la demande de l'autorité compétente

Le destinataire informe l'autorité compétente qui a transmis ou mis à disposition les données à caractère personnel, à sa demande, du traitement de ces données.

Article 16

Information de la personne concernée

1. Les États membres veillent à ce que la personne concernée soit informée de la collecte ou du traitement, par leurs autorités compétentes, de données à caractère personnel la concernant, conformément au droit national.

2. Lorsque des données à caractère personnel ont été transmises ou mises à disposition entre des États membres, chaque État membre peut, conformément aux dispositions de son droit national visées au paragraphe 1, demander que l'autre État membre n'informe pas la personne concernée. Dans ce cas, ce dernier n'informe pas la personne concernée sans l'accord préalable de l'autre État membre.

Article 17

Droit d'accès

1. Toute personne concernée a le droit d'obtenir sur demande formulée à des intervalles raisonnables, sans contrainte et sans délais ni frais excessifs, au moins les informations suivantes:

a) la confirmation du responsable du traitement ou de l'autorité de contrôle nationale que des données la concernant ont été transmises ou mises à disposition et des informations sur les destinataires ou catégories de destinataires auxquels les données ont été communiquées, et la communication des données faisant l'objet du traitement; ou

b) la confirmation de l'autorité de contrôle nationale que toutes les vérifications nécessaires ont eu lieu.

2. Les États membres peuvent adopter des mesures législatives limitant l'accès aux informations visées au paragraphe 1, point a), lorsque cette limitation, tout en tenant dûment compte des intérêts légitimes de la personne concernée, constitue une mesure nécessaire et proportionnée pour:

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

b) 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) protéger la sécurité publique;

d) protéger la sûreté de l'État;

e) protéger la personne concernée ou les droits et libertés d'autrui.

3. Le refus ou la limitation de l'accès sont communiqués par écrit à la personne concernée. Dans le même temps, les raisons matérielles ou juridiques justifiant la décision lui sont également communiquées. Il est possible de renoncer à cette communication pour les raisons visées au paragraphe 2, points a) à e). Dans tous ces cas, la personne concernée est informée qu'elle peut saisir l'autorité de contrôle nationale compétente, une autorité judiciaire ou un tribunal.

Article 18

Droit de rectification, d'effacement ou de verrouillage

1. La personne concernée est en droit d'attendre du responsable du traitement qu'il s'acquitte des tâches qui lui incombent en vertu des articles 4, 8 et 9 en matière de rectification, d'effacement ou de verrouillage de données à caractère personnel qui découlent de la présente décision-cadre. Les États membres établissent si la personne concernée peut faire valoir ce droit directement à l'encontre du responsable du traitement ou par l'intermédiaire de l'autorité de contrôle nationale compétente. Si le responsable du traitement refuse la rectification, l'effacement ou le verrouillage, le refus doit être communiqué par écrit à la personne concernée qui doit être informée des possibilités prévues par la législation nationale pour présenter une réclamation ou un recours juridictionnel. Lorsque la réclamation ou le recours juridictionnel est examiné, il est communiqué à la personne concernée si le responsable du traitement a agi de manière appropriée ou non. Les États membres peuvent aussi prévoir que la personne concernée est informée par l'autorité de contrôle nationale compétente qu'une vérification a eu lieu.

2. Toute donnée à caractère personnel dont l'exactitude est contestée par la personne concernée et dont il ne peut être déterminé si elle est exacte ou non peut être marquée.

Article 19

Droit à réparation

1. Toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente décision-cadre a le droit d'obtenir du responsable du traitement ou d'une autre autorité compétente en vertu de la législation nationale réparation du préjudice subi.

2. Si une autorité compétente d'un État membre a transmis des données à caractère personnel, le destinataire ne peut pas invoquer l'inexactitude des données transmises pour se décharger de la responsabilité qui lui incombe conformément à son droit national à l'égard de la personne lésée. Si le destinataire verse des dommages et intérêts en raison de l'utilisation de données indûment transmises, l'autorité compétente qui a transmis lesdites données en rembourse intégralement le montant au destinataire, en tenant compte de toute erreur éventuellement imputable au destinataire.

Article 20

Voies de recours

Sans préjudice du recours administratif qui peut être prévu avant la saisine de l'autorité judiciaire, la personne concernée doit disposer, en cas de violation des droits qui lui sont garantis par la législation nationale, du droit à un recours juridictionnel.

Article 21

Confidentialité du traitement

1. Les personnes qui ont accès à des données à caractère personnel relevant du champ d'application de la présente décision-cadre peuvent uniquement traiter ces données en tant que membres de l'autorité compétente ou sur instruction de celle-ci, sauf en vertu d'obligations légales.

2. Les personnes travaillant pour une autorité compétente d'un État membre sont liées par toutes les dispositions en matière de protection des données auxquelles l'autorité compétente est soumise.

Article 22

Sécurité des traitements

1. Les États membres font en sorte que les autorités compétentes mettent en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte la transmission de données par l'intermédiaire d'un réseau ou la mise à disposition par l'octroi d'un accès direct automatisé, ainsi que contre toute autre forme de traitement illicite; il convient à cet égard de tenir compte en particulier des risques présentés par le traitement et de la nature des données à protéger. Ces mesures doivent assurer, compte tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

2. En ce qui concerne le traitement automatisé de données, chaque État membre met en œuvre 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 conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).

3. Les États membres font en sorte que ne puissent être désignés que des sous-traitants qui apportent des garanties nécessaires pour ce qui est des mesures techniques et organisationnelles à appliquer conformément au paragraphe 1 et qui respectent les instructions de l'article 21. L'autorité compétente contrôle le sous-traitant à cet égard.

4. Le traitement de données à caractère personnel ne peut être confié à un sous-traitant que sur la base d'un acte juridique ou d'un contrat écrit.

Article 23

Consultation préalable

Les États membres veillent à ce que les autorités de contrôle nationales compétentes soient consultées avant le traitement de données à caractère personnel qui feront partie d'un nouveau fichier à créer si:

a) le traitement concerne certaines catégories de données visées à l'article 6, ou

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

Article 24

Sanctions

Les États membres prennent les mesures appropriées pour assurer la pleine application des dispositions de la présente décision-cadre et définissent notamment les sanctions effectives, proportionnées et dissuasives à appliquer en cas de violation des dispositions prises en application de la présente décision-cadre.

Article 25

Autorités de contrôle nationales

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de conseiller et de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la présente décision-cadre. Ces autorités exercent en toute indépendance les missions dont elles sont investies.

2. Chaque autorité de contrôle dispose notamment:

a) de 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, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements et d'assurer une publication appropriée de ces avis, d'ordonner le verrouillage, 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) du pouvoir d'ester en justice en cas de violation des dispositions nationales adoptées en application de la présente décision-cadre ou du pouvoir de porter cette violation à la connaissance de l'autorité judiciaire. Les décisions de l'autorité de contrôle donnant lieu à des réclamations peuvent faire l'objet d'un recours juridictionnel.

3. Chaque autorité de contrôle peut être saisie par toute personne d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée des suites données à sa demande.

4. Les États membres prévoient que les membres et agents des autorités de contrôle sont liés par les dispositions en matière de protection des données qui s'appliquent à l'autorité compétente concernée, et qu'ils sont soumis, y compris après cessation de leurs activités, à l'obligation du secret professionnel à l'égard des informations confidentielles auxquelles ils ont accès.

Article 26

Lien avec les accords conclus avec des États tiers

La présente décision-cadre ne préjuge pas les obligations et les engagements des États membres ou de l'Union qui découlent d'accords bilatéraux et/ou multilatéraux avec des États tiers en vigueur au moment de l'adoption de la présente décision-cadre.

Dans le cadre de l'application de ces accords, le transfert à un État tiers de données à caractère personnel collectées auprès d'un autre État membre est réalisé dans le respect de l'article 13, paragraphe 1, point c), ou paragraphe 2, selon le cas.

Article 27

Évaluation

1. Le 27 novembre 2013 au plus tard, les États membres font rapport à la Commission sur les mesures nationales qu'ils ont prises pour assurer le plein respect de la présente décision-cadre, et en particulier également pour ce qui est des dispositions qui doivent être respectées dès la collecte des données. La Commission examine notamment l'incidence de ces dispositions relatives au champ d'application de la présente décision-cadre, prévues à l'article 1er, paragraphe 2.

2. La Commission fait rapport au Parlement européen et au Conseil dans un délai d'un an sur les résultats de l'évaluation visée au paragraphe 1 et accompagne son rapport de propositions de modification appropriées à la présente décision-cadre.

Article 28

Relation avec les actes de l'Union adoptés antérieurement

Lorsque, dans des actes adoptés en vertu du titre VI du traité sur l'Union européenne avant l'entrée en vigueur de la présente décision-cadre et qui régissent l'échange de données à caractère personnel entre États membres ou l'accès des autorités désignées des États membres aux systèmes d'information établis en vertu du traité instituant la Communauté européenne, des conditions spécifiques ont été introduites concernant l'utilisation de ces données par l'État membre destinataire, ces conditions prévalent sur les dispositions de la présente décision-cadre relatives à l'utilisation des données transmises ou mises à disposition par un autre État membre.

Article 29

Transposition

1. Les États membres prennent les mesures nécessaires pour se conformer aux dispositions de la présente décision-cadre avant le 27 novembre 2010.

2. Au plus tard à la même date, les États membres transmettent au secrétariat général du Conseil et à la Commission le texte des dispositions transposant dans leur droit national les obligations qui leur incombent en vertu de la présente décision-cadre, ainsi que les informations relatives aux autorités de contrôle visées à l'article 25. Sur la base de ces informations et d'un rapport écrit de la Commission, le Conseil examine, avant le 27 novembre 2011, dans quelle mesure les États membres se sont conformés aux dispositions de la présente décision-cadre.

Article 30

Entrée en vigueur

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

Fait à Bruxelles, le 27 novembre 2008.

Par le Conseil

La présidente

M. ALLIOT-MARIE