COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 4.10.2005
COM(2005) 475 final

2005/0202 (CNS)

Proposition de

DÉCISION-CADRE DU CONSEIL

relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

{SEC(2005) 1241}

(présentée par la Commission)

EXPOSÉ DES MOTIFS

1) CONTEXTE DE LA PROPOSITION

- **Motivations et objectifs de la proposition**

Le 4 novembre 2004, le Conseil européen a adopté le programme de La Haye visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne.[1] Ce programme invite la Commission à formuler, avant la fin de 2005 au plus tard, des propositions destinées à mettre en œuvre le principe de disponibilité et améliorer l'échange transfrontalier d'informations entre les services répressifs des États membres. Le programme de La Haye souligne que ces propositions doivent respecter des conditions fondamentales strictes en matière de protection des données.

En juin 2005, le Conseil et la Commission ont adopté le plan d'action mettant en œuvre le programme de La Haye.[2] Celui-ci se fonde sur la Communication de la Commission au Conseil et au Parlement européen - Le programme de La Haye: Dix priorités pour les cinq prochaines années. Un partenariat pour le renouveau européen dans le domaine de la liberté, de la sécurité et de la justice[3] Aux termes du plan d'action, la Commission présentera, en 2005, des *propositions relatives (1) à l'établissement d'un principe de disponibilité des informations en matière répressive et (2) à des garanties adéquates et à des droits de recours effectifs pour le transfert des données à caractère personnel aux fins de la coopération policière et judiciaire en matière pénale.* Le 13 juillet 2005, le Conseil (Justice et affaires intérieures) a demandé à la Commission, dans sa déclaration sur la réaction de l'UE aux attentats de Londres[4], de présenter ces propositions pour le mois d'octobre 2005.

La présente décision-cadre vise à garantir la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale entre les États membres de l'Union européenne (TUE, titre VI). Son objectif est d'améliorer cette coopération, en particulier lorsqu'il s'agit de prévenir et de combattre le terrorisme, en respectant strictement des conditions essentielles en matière de protection des données. Le texte garantit le respect des droits fondamentaux, et notamment le droit au respect de la vie privée et à la protection des données à caractère personnel dans toute l'Union européenne, en particulier dans la perspective de la mise en œuvre du principe de disponibilité. Il garantit également que l'échange d'informations pertinentes entre les États membres ne sera pas entravé par les différences de niveau de protection des données dans les États membres.

- **Contexte général**

Conformément à une initiative de l'Italie[5] la protection des données à caractère personnel dans le cadre du troisième pilier a déjà été envisagée en 1998. À l'époque, le Conseil «Justice et affaires intérieures» a adopté le plan d'action dit «de Vienne».[6] Ce dernier indiquait que – vu les problèmes horizontaux qui se posent dans le cadre de la coopération policière et judiciaire

---

1 JO C 53 du 03.03.2005, p. 1.
2 JO C 198 du 12.08.2005, p. 1.
3 COM(2005)184 final, Bruxelles, 10.5.2005.
4 Document de travail du Conseil 11158/1/05 REV 1 JAI 255
5 Document de travail du Conseil 8321/98JAI 15
6 JO C 19 du 23.01.1999, p. 1.

en matière pénale – les possibilités d'harmonisation des règles relatives à la protection des données devaient être examinées dans les deux ans suivant l'entrée en vigueur du traité. Toutefois, en 2001, un projet de résolution sur les règles de protection des données à caractère personnel dans les instruments du troisième pilier de l'Union européenne n'a pas pu être adopté.[7] En juin 2003, la présidence grecque a proposé une série de principes généraux sur la protection des données à caractère personnel dans le cadre du troisième pilier[8] , lesquels s'inspirent de la directive 95/46/CE sur la protection des données et de la Charte des droits fondamentaux de l'Union européenne. En 2005, les autorités nationales chargées de la protection des données des États membres de l'Union européenne et le contrôleur européen de la protection des données (CEPD) ont exprimé leur vif soutien à l'égard d'un nouvel instrument juridique de protection des données à caractère personnel dans le cadre du troisième pilier[9]. Le Parlement européen a recommandé l'harmonisation des règles existantes en matière de protection des données individuelles dans les instruments du troisième pilier, en les regroupant au sein d'un seul instrument qui garantisse un niveau identique de protection des données que celui prévu dans le cadre du premier pilier[10].

Selon le programme de La Haye, l'introduction du principe de disponibilité est lié au respect de conditions fondamentales dans le domaine de la protection des données. Manifestement, le Conseil européen a reconnu que les dispositions relatives à la protection des données en vigueur au niveau européen ne seraient pas suffisantes dans la perspective de la mise en oeuvre du principe de disponibilité, qui pourrait comprendre un accès mutuel ou un accès direct (en ligne) aux bases de données nationales ou l'interopérabilité de celles-ci.

Le souci d'assurer un niveau suffisant de protection des données ressort également d'un accord de coopération signé par sept États membres (Allemagne, Autriche, Belgique, Pays-Bas, Luxembourg, France et Espagne) le 27 mai 2005 à Prüm et recommandé comme modèle pour l'échange d'informations entre les États membres de l'Union en général. Cet accord prévoit, à certaines conditions, de donner aux services répressifs d'une Partie contractante un accès direct automatisé aux données à caractère personnel conservées par une autre Partie contractante. Toutefois, cette forme de coopération n'est pas applicable tant que les dispositions relatives à la protection des données de l'accord ne sont pas transposées dans la législation nationale des Parties.

- **Dispositions en vigueur dans le domaine de la proposition**

La Charte des droits fondamentaux de l'Union européenne[11] reconnaît explicitement le droit au respect de la vie privée (article 7) et le droit à la protection des données à caractère personnel (article 8). Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la

---

7 Document de travail du Conseil 6316/2/05 REV 2 JAI 13

8 2514e réunion du Conseil, Justice et affaires inétrieures, Luxembourg, 5-6 juin 2003, Document du Conseil 9845/03 (Presse 150), p. 32

9 Déclaration et document de synthèse sur les services répressifs et l'échange d'informations dans l'UE, adoptés par la Conférence de printemps des autorités européennes de protection des données, Cracovie, 25-26 avril 2005

10 Point 1 h) d'une proposition de recommandation du Parlement européen à l'intention du Conseil sur l'échange d'informations et la coopération concernant les infractions terroristes (2005/2046(INI)), adoptée le 7 juin 2005

11 JO C 364 du 18.12.2000, p. 1 - 10.

concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

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[12] édicte des règles fondamentales concernant la licéité du traitement de données à caractère personnel ainsi que les droits de la personne concernée. Elle contient des dispositions relatives aux voies de recours, aux responsabilités et aux sanctions, au transfert de données à caractère personnel vers des pays tiers, aux codes de conduite, à des autorités de contrôle particulières et à un groupe de protection, ainsi que des dispositions d'application communautaires. Toutefois, la directive ne s'applique pas aux activités qui échappent au champ d'application du droit communautaire, comme celles prévues par le titre VI du traité sur l'Union européenne (TUE). En conséquence, les États membres sont autorisés à décider eux-mêmes des normes qu'ils jugent appropriées au regard du traitement et de la protection des données. Dans le cadre du titre VI TUE, la protection des données à caractère personnel est régie par différents instruments spécifiques. Il s'agit notamment d'instruments qui instaurent des systèmes d'information communs au niveau européen, comme: la convention d'application de l'accord de Schengen, signée en 1990 et contenant des dispositions spécifiques sur la protection des données applicables au Système d'information Schengen;[13] la convention Europol de 1995[14] et, entre autres, les règles relatives à la transmission de données à caractère personnel par Europol à des États et des instances tiers;[15] la décision créant Eurojust de 2002[16] et les dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel;[17] la Convention sur l'emploi de l'informatique dans le domaine des douanes de 1995, y compris les dispositions relatives à la protection des données à caractère personnel applicables au système d'information des douanes;[18] ainsi que la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne de 2000, et notamment son article 23.[19] En ce qui concerne le système d'information Schengen, il convient de porter une attention particulière à l'établissement, au fonctionnement et à l'utilisation du système d'information Schengen de deuxième génération (SIS II), à propos duquel la Commission a déjà présenté des propositions en vue de l'adoption d'une décision du Conseil[20] et de deux règlements.[21]

En outre, il faut prendre en considération l'article 8 de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe de 1981 (STE n° 108), son protocole additionnel de 2001 concernant les autorités de contrôle et les flux transfrontières de données, ainsi que la recommandation Rec(87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Tous les États membres sont parties à la convention, mais tous ne sont pas parties au protocole additionnel.

---

12 JO L 281 du 23.11.1995, p 31
13 JO C 239 du 22.09.2000, p 19
14 JO C 316 du 27.11.1995, p. 2.
15 JO C 88 du 30.03.1999, p. 1.
16 JO L 63 du 06.03.2002, p 1
17 JO C 68 du 19.03.2005, p. 1.
18 JO C 316 du 27.11.1995, p. 34.
19 JO C 197 du 12.07.2000, p. 1 - 15.
20 COM(2005) 230 final
21 COM(2005)236 final, COM(2005)237 final

- **Cohérence avec les autres politiques et les objectifs de l'Union**

Il convient de reconnaître les particularités du traitement et de la protection des données dans le cadre du titre VI du traité sur l'Union européenne. D'une part, ces spécificités ne doivent pas faire obstacle à la cohérence avec la politique générale de l'Union dans le domaine du respect de la vie privée et de la protection des données sur le fondement de la Charte des droits fondamentaux et de la directive 95/46/CE. Les principes fondamentaux de la protection des données s'appliquent au traitement des données dans le cadre des premier et troisième piliers. D'autre part, la cohérence doit être assurée avec les autres instruments qui prévoient des obligations spécifiques en ce qui concerne les informations susceptibles d'être pertinentes aux fins de la prévention et de la lutte contre la criminalité. Il convient de suivre l'évolution de la situation en ce qui concerne la conservation des données traitées et stockées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou des données transmises sur les réseaux de télécommunications publics aux fins de prévention et de détection des infractions pénales, y compris du terrorisme, et d'enquêtes et de poursuites en la matière. Il convient tout particulièrement de prendre en considération le rapport étroit qui existe entre le présente proposition de décision-cadre et la proposition de la Commission visant à adopter une directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE.[22]

2) CONSULTATION DES PARTIES INTERESSEES ET ANALYSE D'IMPACT

- **Consultation des parties intéressées**

Méthodes de consultation utilisées, principaux secteurs visés et profil général des répondants

Le 22 novembre 2004 et le 21 juin 2005, la Commission a invité et consulté des experts des gouvernements des États membres, de l'Islande, de la Norvège et de la Suisse ainsi que, le 11 janvier 2005, des experts des autorités nationales chargées de la protection des données de ces États. Le CEPD, Europol, Eurojust et le secrétariat des autorités de contrôle communes étaient également représentés. Le but premier de ces consultations était de déterminer si un instrument juridique relatif au traitement et à la protection des données à caractère personnel dans le cadre du troisième pilier était nécessaire et, dans l'affirmative, de définir le principal contenu de cet instrument. La Commission s'est adressée aux parties consultées, notamment sur la base d'un questionnaire et d'un document de réflexion, pour connaître leur position concernant l'approche générale à adopter à propos de la création d'un nouvel instrument juridique et de ses liens avec les instruments existants, de son fondement juridique, de son champ d'application éventuel, des principes régissant la qualité des données, des critères de légitimité du traitement des données par la police ou les autorités judiciaires, des données à caractère personnel des personnes non suspectes, des conditions à remplir pour la transmission de données à caractère personnel aux autorités compétentes d'autres États membres et de pays tiers, des droits de la personne concernée, des autorités de contrôle et d'un éventuel groupe consultatif pour la protection des données dans le cadre du troisième pilier.

Le groupe institué en application de l'article 29 de la directive 95/46/CE a été régulièrement informé de l'évolution du dossier. Le 12 avril et le 21 juin 2005, la Commission a participé à

[22] COM (2005) 438 final, 21.9.2005.

des réunions du groupe de travail «police» de la conférence des autorités européennes de protection des données. Le 31 janvier 2005, la Commission a participé à un séminaire public tenu par la commission des libertés civiles, de la justice et des affaires intérieures sur le thème «Protection des données et sécurité des citoyens: quels principes pour l'Union européenne?». La Commission a tenu compte des résultats de la conférence de printemps des autorités européennes de protection des données (Cracovie, 25-26 avril 2005) et de la position du Parlement européen telle qu'elle apparaît notamment dans sa recommandation au Conseil européen et au Conseil sur l'échange d'informations et la coopération concernant les infractions terroristes (2005/2046(INI)), adoptée le 7 juin 2005.[2]

Synthèse des réponses reçues et de la façon dont elles ont été prises en compte

Tant le Parlement européen que les autorités nationales chargées de la protection des données dans l'Union européenne soutiennent vivement la création d'un instrument juridique sur la protection des données à caractère personnel dans le cadre du troisième pilier. Les représentants des gouvernements des États membres et de l'Islande, de la Norvège et de la Suisse, Europol et Eurojust n'ont pas exprimé de position commune à cet égard. Toutefois, la Commission a pu conclure qu'il n'y avait pas d'opposition majeure à l'idée de créer un tel instrument. Il a semblé y avoir un accord sur le fait que la mise en œuvre du principe de disponibilité doit s'accompagner de règles correctives appropriées dans le domaine de la protection des données. Certains États membres ont indiqué que les modalités d'échange futur des informations devaient être définies au préalable et que les règles relatives à la protection des données à caractère personnel devaient être fixées ultérieurement. D'aucuns ont marqué leur préférence pour l'insertion, dans cet acte, d'une série de dispositions spécifiques sur le principe de disponibilité.

Après avoir examiné les différents points de vue, la Commission est d'avis que la mise en œuvre du principe de disponibilité permettra de développer et de changer radicalement la qualité et l'intensité de l'échange d'informations entre les États membres. Cette évolution aura une incidence majeure sur les données à caractère personnel et le droit à la protection des données. Elle devra s'accompagner de mesures correctives appropriées. Les initiatives récentes visant à établir un accès direct automatisé sont, du moins en termes de réponses positives ou négatives, susceptibles d'accroître le risque d'échange de données illégitimes, inexactes ou obsolètes et doivent être prises en considération. Ces initiatives impliquent que le contrôleur des données ne sera plus en mesure de vérifier *au cas par cas* la légitimité d'une transmission et l'exactitude des données concernées. En conséquence, il doit y avoir des obligations strictes de garantir et de vérifier en permanence la qualité des données pour lesquelles l'accès direct automatisé est autorisé.

Étant donné qu'une attention particulière est accordée à l'impact de la mise en œuvre du principe de disponibilité, les dispositions qui se contentent de régir les aspects individuels de la protection des données ne sont pas suffisantes. Un instrument juridique sur la protection des données à caractère personnel dans le cadre du troisième pilier peut, en principe, contribuer à renforcer la coopération policière et judiciaire en matière pénale du point de vue de son efficacité et de sa légitimité et du respect des droits fondamentaux, notamment du droit à la protection des données à caractère personnel.

Dans la perspective de la mise en oeuvre du principe de disponibilité notamment, un tel instrument est tout particulièrement nécessaire et doit être élaboré tout en mettant en œuvre ce principe. La décision-cadre doit respecter l'esprit et la structure de la directive 95/46/CE dans la mesure du possible, tout en tenant compte des besoins spécifiques de la coopération

policière et judiciaire en matière pénale, à la lumière du principe de proportionnalité. La recommandation Rec(87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, adoptée par le Conseil de l'Europe en 1987, a été prise en considération afin de transposer ses grands principes dans des dispositions contraignantes au niveau de l'UE. Des règles claires doivent être fixées pour la protection des données à caractère personnel qui sont ou seront mises à disposition des autorités compétentes d'autres États membres. Cela implique un système garantissant la qualité du traitement des données en question. Ce système doit inclure des dispositions définissant des droits suffisants pour la personne concernée et les pouvoirs des autorités de contrôle, étant donné que l'exercice de ces droits et pouvoirs peut contribuer à la qualité des données en cause.

- **Analyse d'impact**

Les options suivantes ont été examinées: applicabilité de la directive 95/46/CE; pas de proposition de texte sur la protection des données à caractère personnel dans le cadre du troisième pilier ou proposition ultérieure; ensemble limité de dispositions spécifiques dans un acte normatif concernant l'échange d'informations en application du principe de disponibilité; décision-cadre sur la protection des données à caractère personnel dans le troisième pilier. En ce qui concerne cette dernière option, il s'agissait de déterminer si un tel instrument devait aussi s'appliquer à l'échange d'informations par le biais de systèmes d'information et d'organes établis au niveau de l'UE.

Les dispositions générales et fondamentales de la directive 95/46/CE ne sont pas applicables dans le cadre du troisième pilier comme l'indique son article 3, paragraphe 2. Même la suppression de cet article ne pourrait automatiquement entraîner l'applicabilité de la directive dans le domaine de la coopération policière et judiciaire en matière pénale. Premièrement, les particularités de cette coopération ne sont pas pleinement prises en compte dans la directive et devraient être précisées. Deuxièmement, les exigences relatives à la législation adoptée dans le cadre du titre VI du traité sur l'Union européenne, qui vise à renforcer la coopération policière et judiciaire en matière pénale, doivent être respectées. L'option d'une absence de proposition ou d'une proposition ultérieure concernant des dispositions sur le traitement et la protection des données à caractère personnel dans le cadre du troisième pilier doit être exclue. Il est possible que cette option implique l'introduction de nouvelles formes d'échange d'informations avec la mise en œuvre du principe de disponibilité sans garantir le respect de conditions essentielles strictes dans le domaine de la protection des données. Un ensemble limité de dispositions spécifiques dans un acte normatif concernant l'échange d'informations en application du principe de disponibilité n'est pas suffisant compte tenu de l'impact probable de celui-ci. Une décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale est la seule option pleinement satisfaisante. Il est peu probable que les coûts administratifs engendrés pour les États membres par cette option – si coûts il y a – soient importants.

La Commission a effectué une analyse d'impact qui est mentionnée dans le programme de travail et a publié un rapport à ce sujet sur http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3) ÉLEMENTS JURIDIQUES DE LA PROPOSITION

- **Résumé des mesures proposées**

La décision-cadre proposée inclut des règles générales sur la licéité du traitement des données à caractère personnel, des dispositions concernant des formes spécifiques de traitement (transmission et mise à disposition de données à caractère personnel aux autorités compétentes d'autres États membres, traitement ultérieur, notamment transmission ultérieure, des données reçues d'autorités compétentes d'autres États membres ou mises à disposition par celles-ci), droits de la personne concernée, confidentialité et sécurité du traitement, voies de recours, responsabilité, sanctions, autorités de contrôle et groupe de protection des personnes à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière. Une attention particulière doit être accordée au principe selon lequel les données à caractère personnel ne sont transférées qu'aux pays tiers et aux instances internationales qui garantissent un niveau adéquat de protection. La décision-cadre prévoit un mécanisme visant à assurer le respect de ce principe dans toute l'UE.

- **Base juridique**

La présente décision-cadre se fonde sur les articles 30, 31 et 34, paragraphe 2, point b), du traité sur l'Union européenne. En particulier, compte tenu de la mise en oeuvre du principe de disponibilité, des dispositions appropriées sur le traitement et la protection des données à caractère personnel, y compris des normes communes pour la transmission de ces données à des pays tiers et des instances internationales, sont indispensables pour améliorer la coopération policière et judiciaire en matière pénale, notamment aux fins de la lutte contre le terrorisme et les formes graves de la criminalité. En outre, les États membres ne se feront pleinement confiance que s'il existe des règles communes claires concernant une éventuelle transmission ultérieure des données échangées à d'autres parties, en particulier à des pays tiers. Les dispositions proposées permettront de garantir que l'échange d'informations entre les autorités compétentes n'est pas entravé par les différences de niveau de protection des données dans les États membres.

- **Principes de subsidiarité et de proportionnalité**

La présente décision-cadre régit des situations particulièrement importantes pour la coopération policière et judiciaire en matière pénale entre les États membres, notamment pour l'échange d'informations visant à garantir et à promouvoir l'efficacité et la licéité des mesures destinées à prévenir et combattre la criminalité, en particulier ses formes graves ainsi que le terrorisme, dans *tous* les États membres. Des solutions nationales, bilatérales ou multilatérales peuvent être utiles pour les États membres pris individuellement, mais ne tiendraient pas compte de la nécessité de garantir la sécurité intérieure dans l'ensemble de l'Union. Les besoins d'informations des services répressifs dépendent largement du niveau d'intégration entre les pays. L'échange d'informations à des fins répressives entre les États membres devrait s'intensifier et doit par conséquent s'accompagner de règles cohérentes relatives au traitement et à la protection des données. La présente décision-cadre respecte le principe de subsidiarité tel que visé à l'article 2 du traité sur l'Union européenne et à l'article 5 du traité instituant la Communauté européenne dans la mesure où elle a pour objectif de rapprocher les dispositions législatives et réglementaires des États membres, ce qui ne peut pas être réalisé de manière suffisante par les États membres agissant unilatéralement et suppose une action concertée au niveau de l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé

par ce dernier article, la présente décision-cadre n'excède pas ce qui est nécessaire pour atteindre cet objectif. En particulier, elle ne concerne que le traitement des données à caractère personnel dans la mesure où il a trait à la coopération policière et judiciaire en matière pénale.

- **Choix des instruments**

Instrument proposé: décision-cadre. Cet instrument juridique vise à rapprocher les législations et réglementations des États membres concernant la protection des données à caractère personnel traitées afin de prévenir et de combattre la criminalité.

4) INCIDENCE BUDGETAIRE

La mise en œuvre de la décision-cadre proposée n'entraînerait que des dépenses administratives supplémentaires minimes, à imputer au budget des Communautés européennes, au titre des réunions du comité et du groupe consultatif à instituer en vertu des articles 16 et 31, et de leur appui administratif.

2005/0202 (CNS)

Proposition de

DÉCISION-CADRE DU CONSEIL

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 son article 30, son article 31 et son article 34, paragraphe 2, point b),

vu la proposition de la Commission,[23]

vu l'avis du Parlement européen,[24]

considérant ce qui suit:

(1) L'Union européenne s'est donné pour objectif de maintenir et de développer un espace de liberté, de sécurité et de justice dans l'Union. elle offre aux citoyens un niveau élevé de protection en élaborant une action en commun entre les 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 exigent de traiter les informations pertinentes sous réserve des 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 doit 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 afin de prévenir et de combattre la criminalité peuvent contribuer à atteindre 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 novatrice de l'échange transfrontalier d'informations des services répressifs dans le respect de certaines conditions fondamentales strictes dans

23 …
24 …

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*[25].

(5) L'échange de données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale, notamment de la mise en œuvre du principe de disponibilité des informations au sens du programme de La Haye, doit être étayé par des règles claires et obligatoires qui renforcent la confiance mutuelle entre les autorités compétentes et garantissent que les informations pertinentes sont protégées de manière à exclure toute entrave à cette coopération entre les États membres, tout en respectant pleinement les droits fondamentaux des individus. 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[26] 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 et les activités de l'État en matière pénale.

(6) Un instrument juridique fixant des normes communes pour la protection des données à caractère personnel traitées afin de prévenir et de combattre la criminalité doit être cohérent avec la politique générale de l'Union européenne dans le domaine du respect de la vie privée et de la protection des données. Dans la mesure du possible, compte tenu de la nécessité d'améliorer l'efficacité des activités légitimes de la police, des douanes, des autorités judiciaires et d'autres autorités compétentes, cet instrument doit donc respecter des principes et définitions existants et bien établis, notamment ceux de la directive 95/46/CE du Parlement européen et du Conseil ou ceux relatifs à l'échange d'informations par Europol, Eurojust ou à leur traitement dans le cadre du système d'information des douanes ou d'autres instruments comparables.

(7) Le rapprochement des législations des États membres ne doit pas conduire à affaiblir la protection des données qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans l'Union.

(8) Il convient de préciser les objectifs de la 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 légalité 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 d'autres autorités compétentes ne sauraient être menacées.

(9) La garantie d'un niveau de protection élevé des données à caractère personnel des citoyens européens exige des dispositions communes pour déterminer la légalité et la qualité des données traitées par les autorités compétentes d'autres États membres.

---

[25] JO C 198 du 12.08.2005, p. 1.

[26] JO L 281 du 23.11.1995, p 31

(10) Il est bon de définir au niveau européen les conditions dans lesquelles les autorités compétentes des États membres devraient être autorisées à transmettre les données à caractère personnel à des autorités et des personnes privées dans d'autres États membres et à les mettre à leur disposition.

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

(12) Lorsque des données à caractère personnel sont transférées d'un État membre de l'Union européenne vers des pays tiers ou des instances internationales, ces données devraient, en principe, bénéficier d'un niveau adéquat de protection.

(13) La présente décision-cadre devrait définir la procédure d'adoption des mesures nécessaires pour juger du niveau de protection des données dans un pays tiers ou dans une instance internationale.

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

(15) Il est bon de fixer des règles communes en matière de confidentialité et de sécurité du traitement, de responsabilité et de sanctions pour utilisation illicite par les autorités compétentes, ainsi que de voies de recours offertes à la personne concernée. En outre, il est nécessaire que les États membres prévoient des sanctions pénales pour les infractions particulièrement graves et intentionnelles aux dispositions relatives à la protection des données.

(16) L'établissement, 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.

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

(18) Il conviendrait d'instituer un groupe de protection des personnes à l’égard du traitement des données à caractère personnel aux fins de prévention et de détection des infractions pénales, et d’enquêtes et de poursuites en la matière, qui soit pleinement indépendant dans l'exercice de ses fonctions. Ce groupe aurait pour tâche de conseiller la Commission et les États membres et, en particulier, de contribuer à l'application uniforme des règles nationales adoptées conformément à la présente décision-cadre.

(19) Aux termes de l'article 47 du traité sur l'Union européenne, aucune disposition de ce traité n'affecte 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 comme le prévoit la directive 95/46/CE du Parlement européen et du Conseil, 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[27], 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)[28].

(20) La présente décision-cadre ne porte pas préjudice aux dispositions spécifiques prévues en matière de protection des données par les instruments juridiques pertinents relatifs au traitement et à la protection des données à caractère personnel par Europol, Eurojust et le système d'information des douanes.

(21) Les dispositions relatives à la protection des données à caractère personnel, inscrites au titre IV de la convention d'application de l'Accord de Schengen du 14 juin 1985 relatif à la suppression graduelle des contrôles aux frontières communes[29], signée en 1990 (ci-après «la convention de Schengen»), et intégrées dans le cadre de l'Union européenne en vertu du protocole annexé au traité sur l'Union européenne et au traité instituant la Communauté européenne, devraient être remplacées par les règles de la présente décision-cadre.

(22) Il est bon que la présente décision-cadre s'applique aux données à caractère personnel traitées dans le cadre du système d'information Schengen de deuxième génération et à l'échange d'informations supplémentaires qui y est lié conformément à la décision JAI/2006 …. sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération.

(23) La présente décision-cadre ne porte pas préjudice aux 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[30].

(24) Il est bon de remplacer l'article 23 de la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne[31].

(25) Toute référence relative 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 doit s'entendre comme référence à la présente décision-cadre.

(26) Étant donné que les objectifs de l'action à mener, à savoir la détermination de 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

---

27 JO L 8 du 12.01.2001, p 1.
28 JO L 201 du 31.07.2001, p 37.
29 JO L 239 du 22.09.2000, p 19.
30 JO L 69 du 16.03.2005, p 67.
31 JO C 197 du 12.07.2000, p. 3.

de manière suffisante par les États membres agissant individuellement, et peuvent donc, en raison des dimensions et des effets de l'action envisagée, être mieux réalisés au niveau de l'Union européenne, le Conseil peut arrêter des mesures, conformément au principe de subsidiarité tel qu'il est défini à l'article 5 du traité CE et visé à l'article 2 du traité UE. En vertu du principe de proportionnalité énoncé à l'article 5 du traité CE, la présente décision-cadre n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(26) Le Royaume-Uni participe à la présente décision-cadre en vertu de l'article 5 du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne annexé au traité UE et au traité CE et de 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[32].

(27) L'Irlande participe à la présente décision-cadre en vertu de l'article 5 du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne annexé au traité UE et au traité CE et de 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.

(29) 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 oeuvre, à l'application et au développement de l'acquis de Schengen, qui relèvent du domaine visé à l'article 1er, point H, de la décision 1999/437/CE du Conseil du 17 mai 1999 relative à certaines modalités d'application dudit accord[33].

(30) En ce qui concerne la Suisse, la présente décision 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, qui relève du domaine visé à l'article 1er, point H, de la décision 1999/437/CE du Conseil du 17 mai 1999 en liaison avec l'article 4, paragraphe 1, de la décision 2004/849/CE du Conseil relative à la signature, au nom de l'Union européenne, et à l'application provisoire de certaines dispositions de cet accord[34].

(31) La présente décision-cadre constitue un acte fondé sur l'acquis de Schengen ou qui s'y rapporte, au sens de l'article 3, paragraphe 1, de l'acte d'adhésion de 2003.

(32) 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. Elle tend à assurer le respect des droits au respect de la vie privée et à la protection des données à caractère personnel inscrits aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne,

---

32 JO L 131 du 01.06.2000, p 43.
33 JO L 176 du 10.07.1999, p 31.
34 JO L 368 du 15.12.2004, p 26.

A ARRÊTÉ LA PRÉSENTE DÉCISION-CADRE:

CHAPITRE I OBJET, DÉFINITIONS ET CHAMP D'APPLICATION

Article premier
Objet

1. La présente décision-cadre fixe des normes communes visant à assurer la protection des personnes physiques à l'égard du 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.

2. Les États membres veillent à ce que la divulgation de données à caractère personnel aux autorités compétentes des autres États membres ne soit ni restreinte, ni interdite pour des motifs liés à la protection des données à caractère personnel telle que prévue 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 (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» (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) «fichier de données à caractère personnel» (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;

(d) «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; lorsque les finalités et les moyens du traitement sont définis par le droit national ou par la législation adoptée conformément au titre VI du traité sur l'Union européenne, le responsable du traitement peut être désigné, ou les critères spécifiques relatifs à sa

nomination peuvent être définis, par la législation nationale ou par la législation adoptée conformément au titre VI du traité sur l'Union européenne;

e) «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;

f) «tiers»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données;

g) «destinataire»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers;

h) «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.

i) «instances internationales»: les instances ou organisations établies par des conventions internationales;

j) «autorités compétentes»: les forces de police, les autorités douanières, judiciaires et les autres autorités compétentes dans les États membres au sens de l'article 29 du traité sur l'Union européenne.

Article 3
Champ d'application

1. La présente décision-cadre s'applique au traitement pleinement ou partiellement automatisé des données à caractère personnel et au traitement par des moyens non automatiques de données à caractère personnel faisant partie d'un fichier ou destinées à être incorporées à un fichier par une autorité compétente aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière.

2. La présente décision-cadre ne s'applique pas au traitement de données à caractère personnel par:

   – l'Office européen de police (Europol),

   – l'Unité européenne de coopération judiciaire (Eurojust),

   – le système d'information des douanes tel qu'instauré conformément à la convention établie sur la base de l'article K.3 du traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, et à toute modification de celle-ci.

CHAPITRE II
CONDITIONS GÉNÉRALES DE LICÉITÉ DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Article 4
Principes relatifs à la qualité des données

1. Les États membres font en sorte que les données à caractère personnel soient:

   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. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées;

   c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;

   d) exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées. Les États membres peuvent prévoir un traitement des données selon divers degrés d'exactitude et de fiabilité, auquel cas ils doivent prévoir que les données sont classées selon leur degré d'exactitude et de fiabilité, et notamment que les données fondées sur des faits soient distinguées des données fondées sur des opinions ou appréciations personnelles;

   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 ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1.

3. Les États membres sont tenus de distinguer clairement les données à caractère personnel se rapportant à:

   – une personne soupçonnée d'être l'auteur d'une infraction pénale ou d'avoir participé à une telle infraction,

   – une personne condamnée pour une infraction pénale,

   – une personne au sujet de laquelle on a de bonnes raisons de croire qu'elle commettra une infraction pénale,

   – une personne susceptible d'être appelée à témoigner dans le cadre d'enquêtes relatives à des infractions pénales ou dans des procédures pénales ultérieures,

– une personne victime d'une infraction pénale ou au sujet de laquelle certains faits donnent à croire qu'elle pourrait être victime d'une infraction pénale,

– une personne pouvant fournir des renseignements sur des infractions pénales,

– une personne avec qui l'une des personnes mentionnées ci-dessus a été en contact ou associée, et

– une personne qui ne relève d'aucune des catégories visées ci-dessus.

4. Les États membres prévoient que le traitement des données à caractère personnel n'est nécessaire que si

– il y a de bonnes raisons de croire, à la lumière de faits établis, que les données à caractère personnel concernées rendraient possible, faciliteraient ou accéléreraient la prévention et la détection des infractions pénales, et les enquêtes et poursuites en la matière,

– il n'existe pas d'autre moyen qui affecte moins la personne concernée et

– le traitement des données n'est pas disproportionné par rapport à l'infraction en cause.

Article 5
Critères relatifs à la licéité du traitement des données

Les États membres font en sorte que les données à caractère personnel ne puissent être traitées par les autorités compétentes qu'en vertu d'une loi établissant que ce traitement est nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée et aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière.

Article 6
Traitements portant sur des catégories particulières de données

1. Les États membres interdisent 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.

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

– le traitement est prévu par un texte de loi et absolument nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière, ou si la personne concernée a expressément consenti au traitement, et

– les États membres prévoient des garanties spécifiques appropriées, par exemple l'accès aux données concernées uniquement par le personnel chargé de l'accomplissement des tâches légitimes qui justifient ce traitement.

Article 7
Durée de conservation des données à caractère personnel

1. Les États membres font en sorte que les données à caractère personnel soient conservées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées, sauf disposition contraire du droit national. Les données à caractère personnel des personnes visées à l'article 4, paragraphe 3, dernier tiret, sont conservées dans la limite de la durée strictement nécessaire à la réalisation de la finalité pour laquelle elles sont collectées.

2. Ils mettent en place les mesures procédurales et techniques appropriées garantissant que les durées de conservation des données à caractère personnel sont respectées. Le respect de ces durées de conservation est régulièrement contrôlé.

CHAPITRE III – Formes spécifiques de traitement

SECTION I – TRANSMISSION DE DONNEES A CARACTERE PERSONNEL, Y COMPRIS LEUR MISE A DISPOSITION, AUX AUTORITES COMPETENTES DES AUTRES ÉTATS MEMBRES

Article 8
Transmission de données à caractère personnel, y compris leur mise à disposition, aux autorités compétentes des autres États membres

Les États membres font en sorte que les données à caractère personnel ne soient transmises aux autorités compétentes des autres États membres, ou mises à leur disposition, que si cela est nécessaire pour l'accomplissement des tâches légitimes de l'autorité transmettrice ou réceptrice aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière.

Article 9
Vérification de la qualité des données transmises ou mises à disposition

1. Les États membres font en sorte que la qualité des données à caractère personnel soit vérifiée au plus tard avant la transmission ou la mise à disposition de celles-ci. Dans la mesure du possible, les décisions de justice et les décisions d'arrêt des poursuites doivent être indiquées lors de toute transmission de données, les données fondées sur des opinions ou des appréciations personnelles doivent être vérifiées à la source avant d'être transmises et leur degré d'exactitude ou de fiabilité doit être précisé.

2. Les États membres font en sorte que la qualité des données à caractère personnel, qui sont mises à disposition des autorités compétentes des autres États membres par accès direct automatisé, soit régulièrement vérifiée pour garantir un accès à des données exactes et mises à jour.

3. Les États membres font en sorte que les données à caractère personnel qui ne sont plus exactes ou à jour ne soient pas transmises ou mises à disposition.

4. Les États membres font en sorte qu'une autorité compétente qui a transmis des données à caractère personnel à une autorité compétente d'un autre État membre, ou les a mis à sa disposition, informe cette dernière immédiatement si elle établit, de sa propre initiative ou à la demande de la personne concernée, que les données en question n'auraient pas dû être transmises ou mises à disposition ou que des données inexactes ou obsolètes ont été transmises ou mises à disposition.

5. Les États membres font en sorte qu'une autorité compétente informée conformément au paragraphe 4 supprime ou rectifie les données concernées. En outre, cette autorité rectifie les données concernées si elle détecte que ces données sont inexactes. Si cette autorité a de bonnes raisons de croire que les données à caractère personnel reçues sont inexactes ou doivent être effacées, elle informe sans retard l'autorité compétente qui a transmis ou mis à disposition les données en question.

6. Sans préjudice de la procédure pénale nationale, les États membres font en sorte que les données à caractère personnel soient «annotées» à la demande de la personne concernée si leur exactitude est niée par celle-ci et si leur exactitude ou inexactitude ne peut être vérifiée. Cette «annotation» n'est effacée qu'avec le consentement de la personne concernée ou sur le fondement d'une décision de la juridiction compétente ou de l'autorité de contrôle compétente.

7. Les États membres font en sorte que les données à caractère personnel reçues de l'autorité d'un autre État membre soient effacées

   – si ces données n'auraient pas dû être transmises, mises à disposition ou reçues,

   – à l'expiration d'un délai fixé par la législation de l'autre État membre, si l'autorité qui a transmis ou mis à disposition les données en question a informé l'autorité réceptrice de ce délai lorsque les données ont été transmises ou mises à disposition, sauf si ces données restent nécessaires à des fins de procédure judiciaire,

   – si ces données ne sont pas ou plus nécessaires pour la finalité spécifique pour laquelle elles ont été transmises ou mises à disposition.

8. Si les données à caractère personnel ont été transmises en l'absence de demande, l'autorité réceptrice vérifie sans retard si ces données sont nécessaires pour la finalité pour laquelle elles ont été transmises.

9. Les données à caractère personnel ne sont pas effacées, mais verrouillées conformément à la législation nationale s'il y a de bonnes raisons de croire que leur suppression pourrait affecter les intérêts de la personne concernée dignes de protection. Les données verrouillées ne sont utilisées ou transmises que pour la finalité pour laquelle elles n'ont pas été effacées.

Article 10
Journalisation et enregistrement d'une trace documentaire

1. Les États membres font en sorte que chaque transmission et chaque réception automatisées de données à caractère personnel, en particulier par accès direct automatisé, soient enregistrées dans un journal afin de permettre la vérification

ultérieure des motifs justifiant la transmission, des données transmises, du jour et de l'heure de la transmission, des autorités concernées et, dans la mesure où l'autorité réceptrice est concernée, des personnes ayant reçu les données et des personnes ayant été à l'origine de leur réception.

2. Les États membres font en sorte qu'une trace documentaire soit conservée de chaque transmission et de chaque réception non automatisées de données à caractère personnel afin de permettre la vérification ultérieure des motifs justifiant la transmission, des données transmises, du jour et de l'heure de la transmission, des autorités concernées et, dans la mesure où l'autorité réceptrice est concernée, des personnes ayant reçu les données et des personnes ayant été à l'origine de leur réception.

3. L'autorité ayant enregistré dans un journal ces informations ou en ayant conservé une trace documentaire les communique immédiatement à l'autorité de contrôle compétente à la demande de cette dernière. Ces informations ne sont utilisées que pour contrôler la protection des données et pour garantir le traitement approprié des données ainsi que leur intégrité et leur sécurité.

SECTION II – TRAITEMENT ULTERIEUR, NOTAMMENT TRANSMISSION ET TRANSFERT ULTERIEURS, DE DONNEES REÇUES DES AUTORITES COMPETENTES DES AUTRES ÉTATS MEMBRES OU MISES A DISPOSITION PAR CELLES-CI

Article 11

Traitement ultérieur de données à caractère personnel reçues des autorités compétentes des autres États membres ou mises à disposition par celles-ci

1. Les États membres font en sorte que les données à caractère personnel reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle-ci ne fassent l'objet d'un traitement ultérieur, conformément à la présente décision-cadre, notamment ses articles 4, 5 et 6, que

   a) pour la finalité spécifique pour laquelle elles ont été transmises ou mises à disposition, ou

   b) si nécessaire à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations.

2. Les données à caractère personnel concernées ne font l'objet d'un traitement ultérieur pour les finalités visées au paragraphe 1, point b), qu'avec le consentement préalable de l'autorité qui a transmis les données personnelles ou les a mises à disposition.

3. Le paragraphe 1, point b), ne s'applique pas si une législation spécifique adoptée en vertu du titre VI du traité sur l'Union européenne dispose expressément que les

données à caractère personnel reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle-ci ne font l'objet d'un traitement ultérieur que pour les finalités pour lesquelles elles ont été transmises ou mises à disposition.

Article 12
Transmission à d'autres autorités compétentes

Les États membres font en sorte que les données à caractère personnel reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle-ci ne soient ensuite transmises à leurs autres autorités compétentes ou mises à leur disposition que si l'ensemble des conditions suivantes sont réunies:

a) la transmission ou la mise à disposition fait l'objet d'une obligation ou d'une autorisation légale claire;

b) la transmission ou la mise à disposition est nécessaire à l'accomplissement des tâches légitimes de l'autorité qui a reçu les données en cause ou de l'autorité à qui elles seront ensuite transmises;

c) la transmission ou la mise à disposition est nécessaire pour atteindre la finalité spécifique pour laquelle les données ont été transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations;

d) l'autorité compétente de l'État membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les transmettre ou les mettre à disposition, ou les ayant mises à la disposition de celle-ci, a donné son consentement préalable à leur transmission ou leur mise à disposition ultérieure.

Article 13
Transmission à des autorités autres que les autorités compétentes

Les États membres font en sorte que les données à caractère personnel reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle-ci ne soient ensuite transmises à des autorités, autres que leurs autorités compétentes, que dans des cas déterminés et si l'ensemble des conditions suivantes sont réunies:

a) la transmission fait l'objet d'une obligation ou d'une autorisation légale claire;

b) la transmission

est nécessaire pour atteindre la finalité spécifique pour laquelle les données ont été transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations;

ou

est nécessaire parce que les données concernées sont indispensables pour permettre à l'autorité à laquelle ces données seront transmises ensuite d'accomplir les tâches légales qui lui sont propres, et pour autant que l'objectif de la collecte ou du traitement que doit effectuer cette autorité ne soit pas incompatible avec le traitement prévu à l'origine et que les obligations légales de l'autorité compétente qui a l'intention de transmettre les données ne s'y opposent pas,

ou

est, sans aucun doute, dans l'intérêt de la personne concernée et si celle-ci y a consenti ou si les circonstances permettent de présumer sans équivoque un tel consentement;

c) l'autorité compétente de l'État membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les transmettre, ou les ayant mises à la disposition de celle-ci, a donné son consentement préalable à leur transmission ultérieure.

Article 14
Transmission à des personnes privées

Sans préjudice des règles nationales de procédure pénale, les États membres font en sorte que les données à caractère personnel reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle-ci ne soient ensuite transmises à des personnes privées dans un État membre que dans des cas déterminés et si l'ensemble des conditions suivantes sont réunies:

a) la transmission fait l'objet d'une obligation ou d'une autorisation légale claire;

b) la transmission est nécessaire pour atteindre la finalité pour laquelle les données concernées ont été transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations;

c) l'autorité compétente de l'État membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les transmettre, ou les ayant mises à la disposition de celle-ci, a donné son consentement préalable à leur transmission ultérieure à des personnes privées.

Article 15
Transfert aux autorités compétentes de pays tiers ou à des instances internationales

1. Les États membres font en sorte que les données à caractère personnel reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle-ci ne soient pas transférées ensuite aux autorités compétentes de pays tiers ou à des

instances internationales, sauf si ce transfert est conforme à la présente décision-cadre et, notamment, si l'ensemble des conditions suivantes sont réunies:

a) le transfert fait l'objet d'une obligation ou d'une autorisation légale claire;

b) le transfert est nécessaire pour atteindre la finalité pour laquelle les données concernées ont été transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations;

c) l'autorité compétente d'un autre État membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les transmettre, ou les ayant mises à la disposition de celle-ci a donné son consentement préalable à leur transfert ultérieur;

d) un niveau adéquat de protection des données est assuré dans le pays tiers ou par l'instance internationale auxquels les données concernées seront transférées.

2. Les États membres font en sorte que le caractère adéquat du niveau de protection offert par un pays tiers ou une instance internationale s'apprécie au regard de toutes les circonstances entourant chaque transfert ou catégorie de transferts. En particulier, cette appréciation se fait sur la base d'un examen des éléments suivants: le type de données, les finalités et la durée du traitement en vue duquel les données sont transférées, le pays d'origine et le pays de destination finale, les dispositions légales générales et sectorielles en vigueur dans le pays tiers ou applicables à l'instance concernée, les règles professionnelles et mesures de sécurité qui y sont appliquées, ainsi que l'existence de garanties suffisantes mises en place par le destinataire du transfert.

3. Les États membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers ou une instance internationale n'assurent pas un niveau de protection adéquat au sens du paragraphe 2.

4. Lorsqu'il est établi, conformément à la procédure prévue à l'article 16, qu'un pays tiers ou une instance internationale n'assure pas un niveau de protection adéquat au sens du paragraphe 2, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de données à caractère personnel vers le pays tiers ou l'instance internationale en cause.

5. Il peut être établi, conformément à la procédure prévue à l'article 16, qu'un pays tiers ou une instance internationale assure un niveau de protection adéquat au sens du paragraphe 2, en raison de sa législation interne ou de ses engagements internationaux, pour ce qui est de la protection de la vie privée et des libertés et droits fondamentaux des personnes.

6. À titre exceptionnel, les données à caractère personnel reçues de l'autorité compétente d'un autre État membre peuvent ensuite être transférées aux autorités compétentes de pays tiers ou à des instances internationales n'assurant pas un niveau

adéquat de protection ou au sein desquelles ce niveau de protection n'est pas assuré, en cas d'absolue nécessité afin de sauvegarder les intérêts essentiels d'un État membre, ou à des fins de prévention de menaces imminentes graves à l'encontre de la sécurité publique ou d'une ou de plusieurs personnes en particulier.

Article 16

Comité

1. Lorsqu'il est fait référence au présent article, la Commission est assistée d'un comité composé de représentants des États membres et présidé par un représentant de la Commission.

2. Le comité adopte son règlement intérieur, sur proposition du président, sur la base du règlement intérieur type publié au *Journal officiel de l'Union européenne*.

3. Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet, dans un délai que le président peut fixer en fonction de l'urgence de la question en cause. L'avis est émis à la majorité prévue à l'article 205, paragraphe 2, du traité instituant la Communauté européenne pour l'adoption des décisions que le Conseil est appelé à prendre sur proposition de la Commission. Lors des votes au sein du comité, les voix des représentants des États membres sont affectées de la pondération définie à l'article précité. Le président ne prend pas part au vote.

4. La Commission arrête les mesures envisagées lorsqu'elles sont conformes à l'avis du comité. Lorsque les mesures envisagées ne sont pas conformes à l'avis du comité, ou en l'absence d'avis, la Commission soumet sans tarder au Conseil une proposition relative aux mesures à prendre et en informe le Parlement européen.

5. Le Conseil peut statuer à la majorité qualifiée sur la proposition, dans un délai de deux mois à compter de sa saisine.

   Si, dans ce délai, le Conseil a indiqué, à la majorité qualifiée, qu'il s'oppose à la proposition, la Commission réexamine celle-ci. Elle peut soumettre au Conseil une proposition modifiée, soumettre à nouveau sa proposition ou présenter une proposition législative. Si, à l'expiration de ce délai, le Conseil n'a pas adopté les mesures d'application proposées ou s'il n'a pas indiqué qu'il s'opposait à la proposition de mesures d'application, les mesures d'application proposées sont arrêtées par la Commission.

Article 17
Dérogations aux articles 12, 13, 14 et 15

Les articles 12, 13, 14 et 15 ne s'appliquent pas si une législation spécifique adoptée en vertu du titre VI du traité sur l'Union européenne dispose expressément que les données à caractère personnel reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle-ci ne doivent pas être transmises ultérieurement ou ne sont transmises ultérieurement que sous réserve du respect de conditions plus précises.

Article 18
Information relative à une demande de l'autorité compétente

Les États membres font en sorte que l'autorité compétente de laquelle des données à caractère personnel ont été reçues ou qui les a mises à disposition soit informée à sa demande du traitement ultérieur de ces données et des résultats obtenus.

CHAPITRE IV
DROITS DE LA PERSONNE CONCERNÉE

Article 19
Droit à l'information lorsque des données sont collectées auprès de la personne concernée et qu'elle en a connaissance

1. Les États membres font en sorte que le responsable du traitement ou son représentant fournisse gratuitement, à la personne auprès de laquelle il collecte des données la concernant et qui en a connaissance, au moins les informations énumérées ci-dessous, sauf si la personne dispose déjà de ces informations:

   a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

   b) les finalités du traitement auquel les données sont destinées;

   c) toute information supplémentaire telle que:

   – la base juridique du traitement,

   – les destinataires ou les catégories de destinataires des données,

   – le caractère obligatoire ou facultatif de la réponse aux questions ou d'autres formes de coopération, ainsi que les conséquences éventuelles d'un défaut de réponse ou de coopération;

   – l'existence d'un droit d'accès aux données la concernant et de rectification de ces données

   dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

2. La fourniture des informations énumérées au paragraphe 1 est refusée ou limitée uniquement si cela s'avère nécessaire

   a) pour permettre au responsable du traitement d'accomplir ses tâches légales de manière satisfaisante,

   b) pour éviter de compromettre des enquêtes, recherches ou procédures en cours, ou de nuire à l'accomplissement par les autorités compétentes de leurs tâches légales,

c) pour protéger la sécurité publique et l'ordre public dans un État membre,

d) pour protéger les droits et libertés des tiers,

sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations.

3. Si la fourniture des informations visées au paragraphe 1 est refusée ou limitée, le responsable du traitement informe la personne concernée qu'elle peut introduire un recours devant l'autorité de contrôle compétente, sans préjudice d'éventuels recours juridictionnels et procédures pénales nationales.

4. Les motifs justifiant un refus ou une limitation en application du paragraphe 2 ne sont pas communiqués si leur communication compromet la finalité du refus. En pareil cas, le responsable du traitement informe la personne concernée qu'elle peut introduire un recours devant l'autorité de contrôle compétente, sans préjudice d'éventuels recours juridictionnels et procédures pénales nationales. Si la personne concernée forme un recours auprès de l'autorité de contrôle, cette dernière examine ce recours. Lorsqu'elle examine le recours, l'autorité de contrôle fait simplement savoir à la personne concernée si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées.

Article 20

Droit à l'information lorsque les données n'ont pas été collectées auprès de la personne concernée ou ont été obtenues de sa part sans qu'elle en ait connaissance

1. Lorsque les données n'ont pas été collectées auprès de la personne concernée ou ont été obtenues de sa part sans qu'elle ait connaissance ou conscience du fait que des données étaient collectées à son sujet, les États membres font en sorte que le responsable du traitement ou son représentant fournisse gratuitement à la personne concernée, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, dans un délai raisonnable après la première communication de données, au moins les informations énumérées ci-dessous, sauf si la personne concernée dispose déjà de ces informations ou si la fourniture d'informations s'avère impossible ou impliquerait un effort disproportionné:

a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

b) les finalités du traitement;

c) toute information supplémentaire telle que:

– la base juridique du traitement,

– les catégories de données concernées,

– les destinataires ou les catégories de destinataires des données,

– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont traitées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

2. Les informations énumérées au paragraphe 1 ne sont pas fournies si cela s'avère nécessaire

a) pour permettre au responsable du traitement d'accomplir ses tâches légales de manière satisfaisante,

b) pour éviter de compromettre des enquêtes, recherches ou procédures en cours, ou de nuire à l'accomplissement par les autorités compétentes de leurs tâches légales,

c) pour protéger la sécurité publique et l'ordre public dans un État membre,

d) pour protéger les droits et libertés des tiers,

sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations.

Article 21
Droit d'accès, de rectification, d'effacement ou de verrouillage

1. Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement:

a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs:

– la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte, sa base juridique et les destinataires ou les catégories de destinataires auxquels les données sont communiquées,

– la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données,

b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente décision-cadre, notamment en raison du caractère incomplet ou inexact des données;

c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point b), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné.

2. Tout acte auquel la personne concernée peut prétendre conformément au paragraphe 1 est refusé si cela s'avère nécessaire

a) pour permettre au responsable du traitement d'accomplir ses tâches légales de manière satisfaisante,

b) pour éviter de compromettre des enquêtes, recherches ou procédures en cours, ou de nuire à l'accomplissement par les autorités compétentes de leurs tâches légales,

c) pour protéger la sécurité publique et l'ordre public dans un État membre,

d) pour protéger les droits et libertés des tiers,

sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations.

3. Tout refus, ou toute limitation, des droits visés au paragraphe 1 est formulé par écrit. Si le droit visé au paragraphe 1 est refusé ou limité, le responsable du traitement informe la personne concernée qu'elle peut introduire un recours devant l'autorité de contrôle compétente, sans préjudice d'éventuels recours juridictionnels et procédures pénales nationales.

4. Les motifs justifiant un refus en application du paragraphe 2 ne sont pas communiqués à la personne concernée si leur communication compromet la finalité du refus. En pareil cas, le responsable du traitement informe la personne concernée qu'elle peut introduire un recours devant l'autorité de contrôle compétente, sans préjudice d'éventuels recours juridictionnels et procédures pénales nationales. Si la personne concernée forme un recours auprès de l'autorité de contrôle, cette dernière examine ce recours. Lorsqu'elle examine le recours, l'autorité de contrôle fait simplement savoir à la personne concernée si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées.

Article 22
Information des tiers à la suite d'une rectification, d'un verrouillage ou d'un effacement

Les États membres font en sorte que des mesures techniques appropriées soient prises pour garantir que, lorsque le responsable du traitement rectifie, verrouille ou efface sur demande des données à caractère personnel, une liste des fournisseurs et des destinataires de ces données est automatiquement établie. Le responsable du traitement veille à ce que les fournisseurs et destinataires figurant sur la liste soient informés des modifications apportées aux données à caractère personnel.

CHAPITRE V
Confidentialité et sécurité du traitement

Article 23
Confidentialité

Toute personne agissant sous l'autorité du responsable du traitement ou du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

Toutes les personnes appelées à travailler avec une autorité compétente d'un État membre ou au sein d'une telle autorité sont liées par des règles strictes de confidentialité.

Article 24
Sécurité

1. Les États membres font en sorte que le responsable du traitement mette en œuvre les mesures techniques et d'organisation 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 des transmissions de données par l'intermédiaire d'un réseau ou des mises à disposition par l'octroi d'un accès direct automatisé, ainsi que contre toute autre forme de traitement illicite, compte tenu, 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. Les mesures sont réputées nécessaires si l'effort qu'elles supposent n'est pas disproportionné par rapport à l'objectif de protection visé.

2. En ce qui concerne le traitement automatisé de données, chaque État membre met en œuvre des mesures conçues pour:

   a) interdire à toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle à l'entrée des 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 dans le fichier ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données à caractère personnel intégrées (contrôle de l'intégration);

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

   e) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès);

   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, 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 ne puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);

i) assurer que les systèmes employés puissent être réparés immédiatement en cas de dérangement (remise en état);

j) assurer que les fonctions du système ne soient pas défectueuses, que les erreurs de fonctionnement soient immédiatement signalées (fiabilité) et que les données stockées ne puissent pas être faussées par une erreur de fonctionnement du système (authenticité).

3. Les États membres font en sorte que le responsable du traitement, lorsque le traitement est effectué pour son compte, choisisse un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer, et qu'il veille au respect de ces mesures.

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

– le sous-traitant n'agit que sur la seule instruction du responsable du traitement,

– les obligations visées aux paragraphes 1 et 2, telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci.

5. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 1 sont consignés par écrit ou sous une autre forme équivalente.

Article 25
Registre

1. Les États membres font en sorte que chaque responsable du traitement tienne un registre des traitements ou séries de traitements poursuivant une même finalité ou des finalités liées. Les renseignements devant figurer dans le registre comprennent notamment

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;

b) la ou les finalités du traitement;

c) une description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;

d) la base juridique du traitement auquel les données sont destinées;

e) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;

f) les transferts de données envisagés à destination de pays tiers;

g) une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application de l'article 24.

2. Les États membres précisent les conditions et modalités de notification à l'autorité de contrôle des informations visées au paragraphe 1.

Article 26
Contrôles préalables

1. Les États membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre.

2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle.

3. Les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées.

CHAPITRE VI
RECOURS JURIDICTIONNELS ET RESPONSABILITE

Article 27
Voies de recours

Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 30, antérieurement à la saisine de l'autorité judiciaire, les États membres font en sorte que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par le droit national applicable au traitement en question en vertu de la présente décision-cadre.

Article 28
Responsabilité

1. Les États membres font en sorte que 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 ait le droit d'obtenir du responsable du traitement réparation du préjudice subi. Le responsable du traitement 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.

2. Toutefois, une autorité compétente qui a reçu des données à caractère personnel de l'autorité compétente d'un autre État membre est responsable à l'égard de la personne lésée des dommages causés en raison de l'utilisation de données inexactes ou obsolètes. Elle ne peut dénier sa responsabilité en arguant avoir reçu d'une autre autorité des données inexactes ou obsolètes. Si l'autorité réceptrice est tenue à réparation pour avoir utilisé des données inexactes que lui avait transmises ou mises à disposition l'autorité compétente d'un autre État membre, cette dernière rembourse à l'autorité réceptrice la totalité du montant payé à titre de dommages-intérêts.

Article 29
Sanctions

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

2. Les États membres font en sorte que les infractions commises intentionnellement et correspondant à des violations graves des dispositions adoptées en application de la présente décision cadre, notamment de ses dispositions sur la confidentialité et la sécurité des traitements, soient passibles de sanctions pénales effectives, proportionnées et dissuasives.

CHAPITRE VII
AUTORITE DE CONTROLE ET GROUPE DE PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 30
Autorité de contrôle

1. Chaque État membre fait en sorte qu'une ou plusieurs autorités publiques soient chargées de contrôler 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 État membre fait en sorte que les autorités de contrôle soient consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel à des fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière.

3. Chaque autorité de contrôle dispose notamment:

   – 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,

– de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 26, 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,

– du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente décision-cadre ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

4. 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.

5. Chaque autorité de contrôle établit à intervalles réguliers un rapport sur son activité. Ce rapport est publié.

6. Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État membre.

7. Les autorités de contrôle coopèrent entre elles ainsi qu'avec les autorités de contrôle instituées en vertu du titre VI du traité sur l'Union européenne et avec le contrôleur européen de la protection des données dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toutes informations utiles.

8. Les États membres font en sorte que les membres et agents de l'autorité de contrôle soient soumis, y compris après cessation de leurs activités, à l'obligation du secret professionnel à l'égard des informations confidentielles auxquelles ils ont accès.

9. Les prérogatives de l'autorité de contrôle ne portent pas atteinte à l'indépendance du pouvoir judiciaire et toute décision prise par cette autorité est sans préjudice de l'exécution des missions légitimes du pouvoir judiciaire dans le cadre de procédures judiciaires.

Article 31

Groupe de protection des personnes à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière

1. Il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel des fins de prévention et de détection des infractions

pénales, et d'enquêtes et de poursuites en la matière, ci-après dénommé «groupe». Ce groupe a un statut consultatif et agit en toute indépendance.

2. Ce groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant du contrôleur européen de la protection des données et d'un représentant de la Commission.

Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un État membre a désigné plusieurs autorités de contrôle, celles-ci nomment un représentant commun.

Les présidents des autorités de contrôle communes instituées en application du titre VI du traité sur l'Union européenne sont autorisés à participer ou à être représentés aux réunions du groupe. L'autorité ou les autorités de contrôle désignées par l'Islande, la Norvège et la Suisse sont autorisées à être représentées aux réunions du groupe pour ce qui est des questions liées à l'acquis de Schengen.

3. Le groupe prend ses décisions à la majorité simple des représentants des autorités de contrôle des États membres.

4. Le groupe élit son président. La durée du mandat du président est de deux ans. Le mandat est renouvelable.

5. Le secrétariat du groupe est assuré par la Commission.

6. Le groupe établit son règlement intérieur.

7. Le groupe examine les questions mises à l'ordre du jour par son président, soit à l'initiative de celui-ci, soit à la demande d'un représentant des autorités de contrôle, de la Commission, du contrôleur européen de la protection des données ou des présidents des autorités de contrôle communes.

Article 32

Tâches

1. Le groupe a pour mission:

a) d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de la présente décision-cadre, en vue de contribuer à leur mise en œuvre uniforme,

b) de donner un avis sur le niveau de protection dans les États membres, dans les pays tiers et dans les instances internationales, notamment afin de garantir que les données à caractère personnel sont transférées conformément à l'article 15 aux pays tiers et aux instances internationales qui assurent un niveau adéquat de protection des données,

c) de conseiller la Commission et les États membres sur tout projet de modification de la présente décision-cadre, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés

des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière, ainsi que sur tout autre projet de mesures ayant une incidence sur ces droits et libertés.

2. Si le groupe constate que des divergences, susceptibles de porter atteinte à l'équivalence de la protection des personnes à l'égard du traitement des données à caractère personnel dans l'Union européenne, apparaissent entre les législations et pratiques des États membres, il en informe le Conseil et la Commission.

3. Le groupe peut émettre de sa propre initiative ou à l'initiative de la Commission ou du Conseil des recommandations sur toute question concernant la protection des personnes à l'égard du traitement des données à caractère personnel dans l'Union européenne à des fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière.

4. Les avis et recommandations du groupe sont transmis au Conseil, à la Commission, au Parlement européen et au comité visé à l'article 16.

5. La Commission informe le groupe, sur la base des informations communiquées par les États membres, des suites qu'elle a données à ses avis et recommandations. Elle rédige à cet effet un rapport qui est transmis également au Parlement européen et au Conseil. Ce rapport est publié. Les États membres informent le groupe de toute mesure qu'ils prennent en application du paragraphe 1.

6. Le groupe établit un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière, dans l'Union européenne et dans les pays tiers, qu'il communique à la Commission, au Parlement européen et au Conseil. Ce rapport est publié.

CHAPITRE VIII
Dispositions finales

Article 33
Modification de la convention de Schengen

Pour ce qui est des domaines relevant du traité sur l'Union européenne, la présente décision-cadre remplace les articles 126 à 130 de la convention de Schengen.

Article 34
Rapport avec des instruments existants qui concernent le traitement et la protection des données à caractère personnel

1. La présente décision-cadre remplace l'article 23 de la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne.

2. Toute référence à la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel doit être interprétée comme étant une référence à la présente décision-cadre.

Article 35
Transposition

1. Les États membres adoptent les mesures nécessaires pour se conformer aux dispositions de la présente décision-cadre au plus tard le 31 décembre 2006.

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 à la désignation de l'autorité ou des autorités de contrôle visées à l'article 29. Sur la base de ces informations et d'un rapport écrit de la Commission, le Conseil examine, avant le 31 décembre 2007, dans quelle mesure les États membres ont pris les dispositions nécessaires pour se conformer à la présente décision-cadre.

Article 36
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

Par le Conseil
Le président

ANNEXE

FICHE FINANCIÈRE LÉGISLATIVE

Domaine(s) politique(s): Justice et affaires intérieures

Activité(s): 1806 – Création d'un véritable espace de liberté, de sécurité et de justice en matière pénale et civile

DENOMINATION DE L'ACTION: PROPOSITION DE DECISION-CADRE DU CONSEIL RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL TRAITEES DANS LE CADRE DE LA COOPERATION POLICIERE ET JUDICIAIRE EN MATIERE PENALE

1. LIGNE(S) BUDGÉTAIRE(S) + INTITULÉ(S)

Sans objet.

2. DONNÉES CHIFFRÉES GLOBALES

2.1. Enveloppe totale de l'action (partie B): millions d'euros en CE

Sans objet.

2.2. Période d'application:

Lancement en 2006.

2.3. Estimation globale pluriannuelle des dépenses:

a) Échéancier crédits d'engagement/crédits de paiement (intervention financière) (*cf. point 6.1.1*)

millions d'euros (*à la 3e décimale*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Total
Crédits d'engagement (CE)							
Crédits de paiement (CP)							

b) Assistance technique et administrative (ATA) et dépenses d'appui (DDA) (*cf. point 6.1.2*)

CE							
CP							

Sous-total a+b		

CE							
CP							

c) Incidence financière globale des ressources humaines et autres dépenses de fonctionnement
(cf. points 7.2 et 7.3)

CE/CP	0,389	0,389	0,389	0,389	0,389	0,389	2,334

TOTAL a+b+c							
CE							
CP							

2.4. Compatibilité avec la programmation financière et les perspectives financières

Sans objet.

2.5. Incidence financière sur les recettes

Proposition sans incidence financière.

3. CARACTÉRISTIQUES BUDGÉTAIRES

Nature de la dépense		**Nouvelle**	**Participation AELE**	**Participation pays candidats**	**Rubrique PF**
DNO	CND	Sans objet	Sans objet	Sans objet	**N°** Sans objet

4. BASE JURIDIQUE

Articles 30 et 31, et article 34, paragraphe 2, point b), du traité UE.

5. DESCRIPTION ET JUSTIFICATION

5.1. Nécessité d'une intervention communautaire

5.1.1. Objectifs poursuivis

La proposition de décision-cadre fixe des normes communes concernant la protection des données à caractère personnel traitées par les autorités compétentes dans le cadre d'activités prévues par le titre VI du traité sur l'Union européenne (coopération policière et judiciaire en matière pénale). Des autorités de contrôle publiques et indépendantes vérifient l'application des dispositions nationales prises en vertu de la présente décision-cadre dans les États membres. Au niveau de l'UE, il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, et

d'enquêtes et de poursuites en la matière, ci-après dénommé «groupe». Ce groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant du contrôleur européen de la protection des données, et d'un représentant de la Commission. Il examine toute question portant sur la mise en œuvre des dispositions nationales prises en application de la présente décision-cadre, en vue de contribuer à leur mise en œuvre uniforme. Il rend des avis sur le niveau de protection des données dans les États membres et dans les pays tiers et conseille la Commission et les États membres sur tout projet de modification de la décision-cadre ainsi que sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits fondamentaux.

En outre, conformément à l'article 16 de la décision-cadre, un comité, composé des représentants des États membres et présidé par un représentant de la Commission, aide la Commission à apprécier, si nécessaire, le niveau de protection des données dans un pays tiers.

5.1.2. Dispositions prises relevant de l'évaluation ex ante

Les représentants des gouvernements et des autorités indépendantes de contrôle des États membres, de l'Islande, de la Norvège et de la Suisse, ainsi que le contrôleur européen de la protection des données, Europol et Eurojust ont été consultés. En particulier, compte tenu des différents points de vue, la Commission propose d'instituer le groupe susmentionné. Afin de procéder à une estimation des éventuels coûts entraînés par cette mesure, la Commission a vérifié les coûts (frais de déplacement, appui administratif pour la préparation et l'organisation des réunions) actuellement générés par le groupe de travail institué conformément à l'article 29 de la directive 95/46/CE.

5.2. Actions envisagées et modalités de l'intervention budgétaire

Il est probable que le groupe précité se réunisse régulièrement, le nombre de réunions étant estimé à cinq par an. Le comité visé à l'article 16 se réunira si nécessaire et aussi souvent que nécessaire, jusqu'à cinq fois par an également. Le remboursement se fera sur la base d'un participant par État membre et par État Schengen (Islande, Norvège). Les groupes institués conformément aux articles 29 et 31 de 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, permettent de dégager certaines orientations.

5.3. Modalités de mise en œuvre

Toutes les réunions devront être organisées par la Commission et se dérouler dans ses locaux. La Commission devra fournir des services de secrétariat pour le groupe de travail et le comité précités ainsi que préparer et organiser leurs réunions.

6. INCIDENCE FINANCIÈRE

6.1. Incidence financière totale sur la partie B (pour toute la période de programmation)

6.1.1. Intervention financière

Sans objet.

6.1.2. Assistance technique et administrative (ATA), dépenses d'appui (DDA) et dépenses TI (crédits d'engagement)

Sans objet.

6.2. Calcul des coûts par mesure envisagée en partie B (pour toute la période de programmation)

Sans objet.

7. INCIDENCE SUR LES EFFECTIFS ET LES DÉPENSES ADMINISTRATIVES

L'incidence sur les effectifs et les dépenses administratives sera couverte par les ressources allouées à la DG chef de file dans le cadre de la procédure annuelle d'allocation.

L'attribution de postes dépend aussi de la répartition des fonctions et de l'attribution des ressources dans le cadre des perspectives financières 2007-2013.

7.1. Incidence sur les ressources humaines

Types d'emplois		Effectifs à affecter à la gestion de l'action par utilisation des ressources existantes et/ou supplémentaires		Total	Description des tâches découlant de l'action
		Nombre d'emplois permanents	Nombre d'emplois temporaires		
Fonctionnaires ou agents temporaires	A B C	0,25 A 0,50 B 1,00 C		0,25A 0,50B 1,00C	Assurer un appui administratif, préparer les réunions du groupe et du comité
Autres ressources humaines					
Total					

7.2. Incidence financière globale des ressources humaines

Type de ressources humaines	Montant (€)	Mode de calcul *

Fonctionnaires Agents temporaires	1ère année :189 000	1 X 108 000 0,5 X 108 000 0,25 X 108 000 = 189 000
Autres ressources humaines (indiquer la ligne budgétaire)		
Total	189 000	

Les montants correspondent aux dépenses totales pour 12 mois.

7.3. Autres dépenses de fonctionnement découlant de l'action

Ligne budgétaire (n° et intitulé)	Montants en euros	Mode de calcul
Enveloppe globale (Titre A7) A0701 – Missions A07030 – Réunions A07031 - Comités obligatoires A07032 - Comités non obligatoires A07040 – Conférences A0705 - Études et consultations Autres dépenses (indiquer lesquelles)	200 000	10 réunions* 27 * 740€
Systèmes d'information (A-5001/A-4300)		
Autres dépenses - partie A (indiquer lesquelles)		
Total	200 000	

Les montants correspondent aux dépenses totales pour 12 mois.

Préciser le type de comité ainsi que le groupe auquel il appartient.

I.	Total annuel (7.2 + 7.3)	389 000 euros
II.	Durée de l'action	
III.	Coût total de l'action (I x II)	

8. SUIVI ET ÉVALUATION

8.1. Système de suivi

Le groupe de travail et le comité arrêtent leur règlement intérieur, lequel prévoit notamment des règles en matière de confidentialité. Le Parlement européen sera informé selon des modalités analogues à celles prévues à l'article 7 de la décision 1999/468/CE du Conseil du 28 juin 1999 fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission (JO L 184 du 17.7.1999, p. 23).

8.2. Modalités et périodicité de l'évaluation prévue

Sans objet.

9. MESURES ANTIFRAUDE

Sans objet.

XXX