Conseil de
l'Union européenne

Bruxelles, le 28 janvier 2016
(OR. en)

5463/16

Dossier interinstitutionnel:
2012/0010 (COD)

DATAPROTECT 4
JAI 46
DAPIX 14
FREMP 6
COMIX 40
CODEC 56

NOTE POINT "I/A"

Origine:	la présidence
Destinataire:	Comité des représentants permanents/Conseil
Nº doc. préc.:	15360/15
Objet:	Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données [première lecture] - Accord politique

INTRODUCTION

1. La Commission a présenté, le 25 janvier 2012, un paquet concernant la protection des données, comprenant:

   – une proposition de règlement général sur la protection des données, qui est destinée à remplacer la directive de 1995 sur la protection des données (ex-premier pilier);

   – la proposition de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, visée en objet, qui est destinée à remplacer la décision-cadre de 2008 sur la protection des données (ex-troisième pilier).

2. La directive sur la protection des données a pour objectif d'assurer un niveau élevé et homogène de protection et de faciliter la libre circulation des données à caractère personnel dans le cadre de la coopération judiciaire en matière pénale et de la coopération policière.

3. Le Parlement européen a adopté sa position en première lecture sur la proposition de directive sur la protection des données le 12 mars 2014 (doc. 7428/14).

4. Le Conseil a dégagé une orientation générale (doc. 12555/15) sur la proposition de directive sur la protection des données le 8 octobre 2015, donnant ainsi à la présidence un mandat de négociation pour engager les trilogues avec le Parlement européen.

5. À l'issue de cinq trilogues menés depuis octobre 2015, la présidence et les représentants du Parlement européen, assistés par la Commission, sont parvenus à un accord sur un texte de compromis global.

6. Lors de sa réunion du 16 décembre 2015, le Comité des représentants permanents a approuvé le texte issu du trilogue du 15 décembre.

7. Lors d'une réunion extraordinaire tenue le 17 décembre 2015, la commission LIBE du Parlement européen a procédé à un vote sur le texte ayant fait l'objet d'un accord dans le cadre du trilogue. Le même jour, la présidence du Comité des représentants permanents a reçu une lettre du président de la commission LIBE (doc. 15361/15) indiquant que celui-ci recommanderait à la commission LIBE et à la plénière, sous réserve de mise au point par les juristes-linguistes, d'approuver sans amendements l'accord intervenu dans le cadre du trilogue.

8. Lors de sa réunion du 18 décembre 2015, le Coreper a confirmé le texte en vue de parvenir à un accord (doc. 15360/15).

9. Le Comité des représentants permanents est invité à recommander au Conseil de dégager un accord politique sur le texte de la directive sur la protection des données tel qu'il figure à l'annexe de la présente note.

ANNEXE

Proposition de

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

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

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

vu la proposition de la Commission européenne,

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

vu l'avis du contrôleur européen de la protection des données,[1]

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

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

[1] JO C 192 du 30.6.2012, p. 7.

(2) Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes, respecter leurs libertés et droits fondamentaux, notamment le droit à la protection des données à caractère personnel. Cela devrait contribuer à la réalisation d'un espace de liberté, de sécurité et de justice.

(3) L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. La collecte et le partage de données ont connu une augmentation spectaculaire. Les technologies permettent d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre d'activités telles que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales.

(4) Cette évolution exige de faciliter la libre circulation des données entre les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces au sein de l'Union, et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel. Cela oblige à mettre en place dans l'Union un cadre de protection des données solide et plus cohérent, assorti d'une application rigoureuse des règles.

(5) La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2] s'applique à l'ensemble des activités de traitement des données à caractère personnel dans les États membres, à la fois dans les secteurs public et privé. Elle ne s'applique cependant pas au traitement de données à caractère personnel mis en œuvre "pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire", telles que les activités dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière.

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

(6) La décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[3] s'applique dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière. Son champ d'application se limite au traitement des données à caractère personnel qui sont transmises ou mises à disposition entre les États membres.

(7) Il est crucial d'assurer un niveau élevé et homogène de protection des données à caractère personnel des personnes physiques et de faciliter l'échange de données à caractère personnel entre les autorités compétentes des États membres, afin de garantir l'efficacité de la coopération judiciaire en matière pénale et de la coopération policière. À cette fin, le niveau de protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, devrait être équivalent dans tous les États membres. Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige non seulement de renforcer les droits des personnes concernées et les obligations de ceux qui traitent ces données, mais aussi de conférer, dans les États membres, des pouvoirs équivalents de surveillance et de contrôle de l'application des règles relatives à la protection des données à caractère personnel.

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

(9) Sur cette base, le règlement (UE) …./XXX du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) définit des règles générales visant à protéger les personnes physiques à l'égard du traitement des données à caractère personnel et à garantir la libre circulation de ces données dans l'Union.

---

[3] JO L 350 du 30.12.2008, p. 60.

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

(11) Par conséquent, une directive distincte devrait permettre de répondre à la nature spécifique de ces domaines et de fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Les autorités compétentes en question peuvent inclure non seulement les autorités publiques telles que le pouvoir judiciaire, la police et d'autres autorités répressives mais aussi tout autre organisme ou entité à qui la législation nationale confie l'exercice de l'autorité publique et de prérogatives de puissance publique aux fins de la présente directive. Toutefois, lorsqu'un tel organisme ou une telle entité traite des données à caractère personnel à des fins autres que celles de la présente directive, le règlement (UE) ..../XXX s'applique. Par conséquent, le règlement (UE) ..../XXX s'applique lorsqu'un organisme ou une entité collecte des données à caractère personnel à d'autres fins et les traite pour se conformer à une obligation légale à laquelle il est soumis - par exemple, les établissements financiers conservent à des fins d'enquêtes, de détection ou de poursuites certaines données qu'ils traitent et ne les transmettent aux autorités compétentes nationales que dans des cas spécifiques et en conformité avec la législation nationale. Un organisme ou une entité qui traite des données à caractère personnel pour le compte de ces autorités dans le cadre de la présente directive devrait être lié par un contrat ou un autre acte juridique et par les dispositions applicables au responsable du traitement en vertu de la présente directive, le règlement (UE) ..../XXX continuant de s'appliquer aux activités de traitement ne relevant pas du champ d'application de la présente directive.

(11 *bis*) Les activités menées par la police ou d'autres autorités répressives sont axées principalement sur la prévention et la détection des infractions pénales et les enquêtes et les poursuites en la matière, y compris les activités de police effectuées avant qu'il soit déterminé si un fait constitue ou non une infraction pénale. Il peut également s'agir d'exercer une autorité en prenant des mesures coercitives, par exemple dans le cadre d'activités de police lors de manifestations, de grands événements sportifs et d'émeutes. Parmi les activités menées par les autorités précitées figure également le maintien de l'ordre public lorsque cette mission est confiée à la police ou d'autres autorités répressives, si besoin est, à des fins de protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la société protégés par la loi, et de prévention de telles menaces, susceptibles de déboucher sur une infraction pénale. Les États membres peuvent confier à des autorités compétentes d'autres tâches qui ne sont pas nécessairement menées à des fins de prévention et de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, de sorte que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application de la législation de l'Union, relève du champ d'application du règlement (UE) ..../XXX .

(11 *bis bis*) La notion d'infraction pénale au sens de la présente directive devrait être une notion autonome de la législation de l'Union selon l'interprétation de la Cour de justice de l'Union européenne.

(11 *ter*) Étant donné que la présente directive ne devrait pas s'appliquer au traitement de données à caractère personnel dans le cadre d'une activité ne relevant pas du champ d'application de la législation de l'Union, il convient que les activités liées à la sécurité nationale, les activités des agences ou des services responsables de la sécurité nationale et le traitement de données à caractère personnel par les États membres dans le cadre d'activités relevant du champ d'application du titre V, chapitre 2, du traité sur l'Union européenne ne soient pas considérés comme des activités relevant du champ d'application de la présente directive.

(12) Afin d'assurer le même niveau de protection pour les personnes physiques au moyen de droits juridiquement protégés dans l'ensemble de l'Union et d'éviter que des divergences n'entravent les échanges de données à caractère personnel entre les autorités compétentes, la présente directive devrait prévoir des règles harmonisées pour la protection et la libre circulation des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Le rapprochement des législations des États membres ne devrait pas entraîner un affaiblissement de la protection des données qu'elles assurent mais devrait, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans l'Union. Il convient que les États membres ne soient pas empêchés de prévoir des garanties plus strictes que celles établies en vertu de la présente directive pour la protection des droits et des libertés des personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes.

(13) La présente directive s'applique sans préjudice du principe du droit d'accès du public aux documents officiels. En vertu du règlement (UE) ..../XXX, les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique, par un organisme public ou un organisme privé pour l'exécution d'une mission d'intérêt public peuvent être communiquées par cette autorité ou cet organisme conformément au droit de l'Union ou à la législation de l'État membre dont relève l'autorité publique ou l'organisme public, afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel .

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

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

(15 *bis*) Le règlement (CE) nº 45/2001[4] s'applique au traitement des données à caractère personnel par les institutions, organes, organismes et agences de l'Union. Le règlement (CE) nº 45/2001 et les autres instruments juridiques de l'Union applicables au traitement des données à caractère personnel devraient être adaptés aux principes et aux règles du règlement (UE) ..../XXX.

(15 *ter*) La présente directive n'empêche pas les États membres de définir, dans les dispositions nationales relatives aux procédures pénales, les opérations et les procédures de traitement de données à caractère personnel par les juridictions et les autres autorités judiciaires, notamment en ce qui concerne les données à caractère personnel figurant dans les décisions judiciaires et les documents relatifs aux procédures pénales.

(16) Il y a lieu d'appliquer les principes de protection des données à toute information concernant une personne physique identifiée ou identifiable. Pour déterminer si une personne physique est identifiable, il convient de considérer l'ensemble des moyens raisonnablement susceptibles d'être mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier directement ou indirectement cette personne. Pour établir si des moyens sont raisonnablement susceptibles d'être mis en œuvre afin d'identifier une personne physique, il convient de considérer l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte à la fois des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a donc pas lieu d'appliquer les principes de protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données rendues anonymes pour que la personne concernée ne soit pas ou plus identifiable.

[4] JO L 8 du 12.1.2001, p. 1.

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

(16 *bis bis*) Les données génétiques devraient être définies comme les données à caractère personnel liées aux caractéristiques génétiques d'une personne physique qui sont héréditaires ou ont été acquises et qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne, résultant notamment d'une analyse des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou d'une analyse de tout autre élément permettant d'obtenir des informations équivalentes. Compte tenu du caractère complexe et sensible des informations génétiques, le risque est grand que le responsable du traitement fasse un usage abusif et/ou réutilise des données à diverses fins. Il y a eu lieu d'interdire en principe toute discrimination sur la base de caractéristiques génétiques.

(17) Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui comportent des informations sur l'état de santé physique ou mentale passée, présente ou future de la personne concernée, y compris des informations recueillies lors de l'inscription de la personne et de la prestation de services de soins de santé à ce patient, visées dans la directive 2011/24/UE; un numéro, un symbole ou un élément attribué à un patient pour l'identifier de manière univoque à des fins médicales; des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des données génétiques et des échantillons biologiques; ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro.

(17 *bis*) Tous les États membres sont affiliés à l'Organisation internationale de police criminelle (Interpol). Pour exécuter sa mission, Interpol reçoit, conserve et diffuse des données pour aider les autorités compétentes à prévenir et combattre la criminalité organisée. Il est par conséquent approprié de renforcer la coopération entre l'Union européenne et Interpol en favorisant un échange efficace de données à caractère personnel tout en garantissant le respect des libertés et droits fondamentaux dans le cadre du traitement automatique des données à caractère personnel. Lorsque des données à caractère personnel sont transférées de l'Union européenne vers Interpol, et vers des pays qui ont délégué des membres à Interpol, la présente directive devrait s'appliquer, notamment les dispositions relatives aux transferts internationaux. La présente directive devrait être sans préjudice des règles spécifiques énoncées dans la position commune 2005/69/JAI du Conseil du 24 janvier 2005 relative à l'échange de certaines données avec Interpol[5] et dans la décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II)[6].

[5] JO L 27 du 29.1.2005, p. 61.
[6] JO L 205 du 7.8.2007, p. 63.

(18) Tout traitement de données à caractère personnel doit être licite, loyal et transparent à l'égard des personnes physiques concernées et n'être effectué qu'aux fins spécifiques fixées par la loi. Cela n'interdit pas en soi aux autorités répressives de mener des activités telles que des enquêtes discrètes ou de la vidéosurveillance. Ces activités peuvent être menées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, pour autant qu'elles soient déterminées par la loi et qu'elles constituent une mesure nécessaire et proportionnée dans une société démocratique compte tenu des intérêts légitimes de la personne concernée. Le principe de traitement loyal en matière de protection des données est une notion distincte du droit à un procès équitable défini à l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et à l'article 47 de la charte des droits fondamentaux de l'Union européenne. Les personnes physiques devraient être informées des risques, règles, garanties et droits relatifs au traitement de données à caractère personnel les concernant et des modalités d'exercice de leurs droits en relation avec le traitement. En particulier, les finalités précises du traitement devraient être explicites et légitimes, et déterminées lors de la collecte des données. Les données devraient être adéquates et pertinentes au regard des finalités pour lesquelles elles sont traitées, ce qui exige notamment de veiller à ce que les données collectées ne soient pas excessives, ni conservées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement en vue de leur effacement ou d'un examen périodique. Les États membres devraient établir des garanties appropriées pour les données à caractère personnel conservées pendant des périodes plus longues à des fins d'archivage dans l'intérêt public, à des fins statistiques, scientifiques ou historiques.

(19) Aux fins de la prévention des infractions pénales, et des enquêtes et poursuites en la matière, les autorités compétentes ont besoin de traiter des données à caractère personnel, collectées dans le contexte de la prévention et de la détection d'infractions pénales spécifiques, et des enquêtes et poursuites en la matière et, au-delà de ce contexte, pour acquérir une meilleure compréhension des activités criminelles et établir des liens entre les différentes infractions mises au jour.

(19 *bis*) Afin de préserver la sécurité du traitement et de prévenir tout traitement en violation de la présente directive, il convient que les données à caractère personnel soient traitées de manière à garantir une sécurité et une confidentialité appropriées, et notamment à prévenir l'accès non autorisé à ces données et à l'équipement servant à leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement, en tenant compte de l'état des connaissances ainsi que des coûts de mise en œuvre au regard des risques et de la nature des données à caractère personnel à protéger.

(20) (…)

(20 *bis*) Les données à caractère personnel devraient être collectées pour des finalités déterminées, explicites et légitimes relevant du champ d'application de la présente directive et elles ne devraient pas être traitées à des fins incompatibles avec celles de la prévention et de la détection des infractions pénales, des enquêtes et des poursuites en la matière, ou de l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Si des données à caractère personnel sont traitées par le même responsable du traitement ou un autre à une fin relevant du champ d'application de la présente directive autre que celle pour laquelle elles ont été collectées, ce traitement est compatible à condition qu'il soit autorisé conformément aux dispositions légales applicables et qu'il soit nécessaire et proportionné au regard de cette autre fin.

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

(22) (…)

(23) Le traitement des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière implique nécessairement le traitement de données à caractère personnel concernant différentes catégories de personnes concernées. Il importe donc d'établir une distinction, le cas échéant et dans la mesure du possible, entre les données à caractère personnel concernant différentes catégories de personnes concernées, telles que les suspects, les personnes reconnues coupables d'une infraction pénale, les victimes et les tiers, tels que les témoins, les personnes détenant des informations ou des contacts utiles, et les complices de personnes soupçonnées ou condamnées. Cela ne devrait pas empêcher que s'applique le droit à la présomption d'innocence qui est garanti par la charte des droits fondamentaux de l'Union européenne et par la convention européenne des droits de l'homme, telles qu'elles ont été interprétées respectivement par la Cour de justice de l'Union européenne et par la Cour européenne des droits de l'homme dans leur jurisprudence.

(24) Les autorités compétentes devraient veiller à ce que les données à caractère personnel qui sont inexactes, incomplètes ou qui ne sont plus à jour ne soient pas transmises ou mises à disposition. Afin de garantir à la fois la protection des personnes physiques et l'exactitude, l'exhaustivité ou l'actualité et la fiabilité des données à caractère personnel transmises ou mises à disposition, les autorités compétentes devraient, dans la mesure du possible, ajouter les informations nécessaires dans tous les transferts de données à caractère personnel.

(24 *bis*) Lorsque la présente directive fait référence à la législation d'un État membre, à une base juridique ou à une mesure législative, il ne s'agit pas nécessairement d'un acte législatif adopté par un parlement, sans préjudice des obligations prévues par l'ordre constitutionnel de l'État membre concerné; cependant, la législation de cet État membre, cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, comme l'exige la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme. La législation de l'État membre qui réglemente le traitement des données à caractère personnel relevant du champ d'application de la présente directive devrait préciser au minimum les objectifs, les données à caractère personnel qui feront l'objet d'un traitement, les finalités du traitement et les procédures pour garantir l'intégrité et la confidentialité des données à caractère personnel et les procédures prévues pour la destruction de ces dernières, fournissant ainsi des garanties suffisantes vis-à-vis des risques d'utilisation abusive et du caractère arbitraire.

(24 *ter*) Le traitement de données à caractère personnel effectué par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, devrait couvrir les opérations ou séries d'opérations appliquées à des données ou à des ensembles de données à caractère personnel à ces fins, effectuées à l'aide de procédés automatisés ou non, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, le rapprochement ou l'interconnexion, la limitation du traitement, l'effacement ou la destruction. En particulier, les règles fixées dans la présente directive devraient s'appliquer au transfert de données à caractère personnel aux fins de la présente directive à un destinataire non soumis à celle-ci. Par "destinataire", on devrait entendre une personne physique ou morale, une autorité publique, un service ou tout autre organisme auquel les autorités compétentes communiquent de manière licite les données. Lorsque des données ont été initialement collectées par une autorité compétente pour l'une des fins de la présente directive, le règlement (UE) …/XXX devrait s'appliquer au traitement de ces données à des fins autres que celles prévues par la présente directive lorsqu'un tel traitement est autorisé par le droit de l'Union ou la législation d'un État membre. En particulier, les règles fixées dans le règlement (UE) …/XXX devraient s'appliquer au transfert de données à caractère personnel pour des fins ne relevant pas du champ d'application de la présente directive. Le règlement (UE) ..../XXX devrait s'appliquer au traitement de données à caractère personnel par un destinataire qui n'est pas une autorité compétente au sens de la présente directive ou qui n'agit pas en cette qualité et auquel une autorité compétente communique de manière licite des données à caractère personnel. Dans le cadre de la mise en œuvre de la présente directive, les États membres peuvent aussi préciser plus en détail les modalités d'application des règles du règlement (UE) ..../XXX, sous réserve des conditions fixées dans ledit règlement.

(25) Pour être licite, le traitement des données à caractère personnel visé par la présente directive devrait être nécessaire à l'exécution d'une mission d'intérêt général par une autorité compétente, fondée sur le droit de l'Union ou la législation d'un État membre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Ces activités devraient couvrir la sauvegarde des intérêts vitaux de la personne concernée. Dans le cadre de l'exécution des missions se rapportant à la prévention et à la détection des infractions pénales, aux enquêtes et aux poursuites en la matière ou à l'exécution de sanctions pénales qui leur sont confiées de manière institutionnelle par la loi, les autorités compétentes peuvent demander/ordonner aux personnes physiques de donner suite aux demandes qui leur sont adressées. Dans ce cas, le consentement de la personne concernée (au sens du règlement (UE) .../XXX) ne devrait pas constituer une base juridique par le traitement des données à caractère personnel par les autorités compétentes. En effet, lorsqu'elle est tenue de se soumettre à une obligation légale, la personne concernée ne dispose pas d'une véritable liberté de choix, et sa réaction ne saurait être considérée comme une expression spontanée de sa volonté. Cela ne devrait pas empêcher les États membres de prévoir en droit que la personne concernée peut consentir au traitement de données à caractère personnel la concernant aux fins de la présente directive, par exemple pour des tests ADN dans des enquêtes judiciaires ou le suivi de sa localisation au moyen de dispositifs électroniques dans le cadre de l'exécution de sanctions pénales.

(25 *bis*) Les États membres devraient prévoir que lorsque, dans certaines situations particulières, le droit de l'Union ou la législation de l'État membre applicable à l'autorité compétente qui transmet les données soumet le traitement de données à caractère personnel à des conditions spécifiques, par exemple l'utilisation de codes de traitement, l'autorité compétente qui transmet les données devrait informer le destinataire de ces conditions et de l'obligation de les respecter. À ce titre, il peut être exigé, par exemple, que le destinataire des données ne transmette pas ultérieurement ces données ni ne les utilise à d'autres fins ou qu'il s'abstienne d'informer la personne concernée lorsque le droit à l'information est subordonné à l'autorisation préalable de l'autorité compétente qui transmet les données. Ces obligations s'appliquent également lorsque des données sont transmises par l'autorité compétente à des destinataires dans des pays tiers ou des organisations internationales. Les États membres devraient prévoir que cette autorité n'applique pas aux destinataires dans les autres États membres ou aux institutions, organes et organismes établis en vertu des chapitres IV et V du titre V du traité sur le fonctionnement de l'Union européenne des conditions différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État membre dans lequel l'autorité compétente qui transmet les données est établie.

(26) Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées peut entraîner des risques importants pour ces libertés et droits. Il s'agit notamment des données à caractère personnel qui révèlent l'origine raciale ou ethnique, étant entendu que l'utilisation de l'expression "origine raciale" dans la présente directive n'implique pas que l'Union européenne adhère à des théories visant à établir l'existence de races humaines distinctes. Ces données ne devraient pas faire l'objet d'un traitement, à moins que celui-ci s'accompagne d'une protection appropriée des droits et des libertés de la personne concernée conformément à la loi et soit autorisé dans des cas prévus par la loi; ou, s'il n'est pas déjà autorisé par une telle loi, qu'il soit nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne; ou qu'il porte sur des données manifestement rendues publiques par la personne concernée. Afin d'assurer une protection appropriée des droits et des libertés de la personne concernée, il peut être prévu, par exemple, que les données ne puissent être collectées qu'en rapport avec d'autres données relatives à la personne concernée, que les données collectées doivent être suffisamment sécurisées, que l'accès du personnel de l'autorité compétente aux données soit soumis à des règles plus strictes ou encore que la transmission de ces données soit interdite. Dans les cas où le traitement des données est particulièrement intrusif, il convient également que ce traitement soit autorisé par la loi lorsque la personne concernée a expressément marqué son accord. Toutefois, l'accord de la personne concernée ne devrait pas constituer en soi une base juridique pour le traitement de données à caractère personnel sensibles par les autorités compétentes.

(27) La personne concernée devrait avoir le droit de ne pas faire l'objet d'une décision impliquant l'évaluation de certains aspects personnels la concernant, qui résulterait exclusivement d'un traitement automatisé et qui produirait des effets juridiques défavorables la concernant ou qui l'affecterait de manière sensible. En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, y compris une information spécifique de la personne concernée et le droit d'obtenir une intervention humaine, en particulier d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base de données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux, devrait être interdit, dans les conditions visées aux articles 21 et 52 de la charte des droits fondamentaux de l'Union européenne.

(28) Afin de permettre aux personnes concernées d'exercer leurs droits, toute information leur étant destinée devrait être aisément accessible, notamment sur le site web du responsable du traitement, et facile à comprendre, ce qui nécessite l'utilisation de termes simples et clairs. Ces informations devraient être adaptées aux besoins des personnes vulnérables telles que les enfants.

(29) Des modalités devraient être prévues pour faciliter l'exercice par la personne concernée des droits qui lui sont conférés par les dispositions adoptées en vertu de la présente directive, notamment les moyens de demander sans frais l'accès à ses données, leur rectification, leur effacement et la limitation de leur traitement. Le responsable du traitement devrait être tenu de répondre à la personne concernée dans les meilleurs délais, à moins qu'il n'applique des limitations des droits de la personne concernée conformément aux règles de la présente directive. En outre, si les demandes sont manifestement infondées ou excessives, par exemple lorsque la personne concernée présente de façon répétée des demandes d'information déraisonnables ou fait une utilisation abusive de son droit à l'information, par exemple en fournissant des informations fausses ou trompeuses dans le cadre de sa demande, le responsable du traitement peut exiger le paiement de frais raisonnables ou refuser de donner suite à la demande.

(29 *bis*) Lorsque le responsable du traitement demande que des informations supplémentaires lui soient fournies pour confirmer l'identité de la personne concernée, il convient que ces informations fassent l'objet d'un traitement uniquement pour cette finalité précise et qu'elles ne soient pas conservées pendant une durée excédant celle nécessaire au regard de cette finalité précise.

(30) Les informations suivantes, au moins, devraient être communiquées à la personne concernée: l'identité du responsable du traitement, l'existence du traitement et ses finalités, le droit d'introduire une réclamation et l'existence du droit de demander au responsable du traitement l'accès aux données, la rectification ou l'effacement de ces données ou la limitation de leur traitement. Ces informations pourraient figurer sur le site web de l'autorité compétente. En outre, dans des cas précis et afin de permettre à la personne concernée d'exercer ses droits, cette personne devrait être informée de la base juridique du traitement et de la durée pendant laquelle les données seront conservées, dans la mesure où ces autres informations sont nécessaires pour assurer un traitement loyal des données à l'égard de la personne concernée, compte tenu des circonstances particulières dans lesquelles les données sont traitées.

(31) (…)

(32) Une personne physique devrait avoir le droit d'accéder aux données qui ont été collectées à son sujet et d'exercer ce droit facilement, à des intervalles raisonnables, afin de s'informer du traitement dont ses données font l'objet et d'en vérifier la licéité. En conséquence, chaque personne concernée devrait avoir le droit de connaître et de se faire communiquer en particulier la finalité du traitement des données, la durée de leur conservation, ainsi que l'identité des destinataires, y compris dans des pays tiers. Lorsque cette communication comporte des informations relatives à l'origine des données à caractère personnel, ces informations ne devraient pas révéler l'identité des personnes physiques, en particulier les sources confidentielles. Pour que ce droit soit respecté, il suffit que la personne concernée dispose d'un aperçu complet de ces données sous une forme intelligible, c'est-à-dire une forme qui lui permette de prendre connaissance de ces données et de vérifier si elles sont exactes et traitées conformément à la présente directive, de sorte qu'elle puisse, si nécessaire, exercer les droits que lui confère la présente directive. Cet aperçu pourrait être fourni sous la forme d'une copie des données à caractère personnel faisant l'objet du traitement.

(33) Les États membres devraient être autorisés à adopter des mesures législatives visant à retarder ou à limiter l'information des personnes concernées ou à ne pas leur accorder cette information, ou à limiter, complètement ou partiellement, leur accès aux données à caractère personnel les concernant, dès lors qu'une telle mesure est nécessaire et proportionnée dans une société démocratique, eu égard aux droits fondamentaux et aux intérêts légitimes de la personne concernée, pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, pour éviter de nuire à la prévention et à la détection des infractions pénales, aux enquêtes et poursuites en la matière ou à l'exécution de sanctions pénales, pour sauvegarder la sécurité publique ou la sécurité nationale, ou pour protéger les droits et libertés d'autrui. Le responsable du traitement devrait apprécier, en examinant chaque cas de façon concrète et individuelle, s'il y a lieu de limiter le droit d'accès partiellement ou complètement.

(34) Tout refus d'accès ou toute limitation de l'accès devrait en principe être présenté par écrit à la personne concernée et indiquer les motifs factuels ou juridiques sur lesquels la décision est fondée.

(34 *bis*) Toute limitation des droits de la personne concernée doit être conforme à la charte des droits fondamentaux de l'Union européenne et à la convention européenne des droits de l'homme, telles qu'elles ont été interprétées respectivement par la Cour de justice de l'Union européenne et par la Cour européenne des droits de l'homme dans leur jurisprudence, et notamment respecter le contenu essentiel desdits droits et libertés.

(35) (…)

(36) Une personne physique devrait avoir le droit de faire rectifier des données à caractère personnel inexactes la concernant, en particulier lorsque cela touche aux faits, et disposer d'un droit d'effacement lorsque le traitement n'est pas conforme aux dispositions énoncées dans la présente directive. Cependant, le droit de rectification ne devrait pas affecter, par exemple, la teneur d'une déposition. Une personne physique devrait également avoir le droit d'obtenir la limitation du traitement lorsqu'elle conteste l'exactitude des données à caractère personnel et qu'il ne peut être déterminé si ces données sont exactes ou non, ou lorsque les données à caractère personnel doivent être conservées à des fins probatoires. Plus particulièrement, les données à caractère personnel devraient faire l'objet d'un traitement limité plutôt qu'être effacées si, dans un cas donné, il existe des motifs raisonnables de penser que l'effacement pourrait nuire aux intérêts légitimes de la personne concernée. En pareil cas, les données faisant l'objet d'un traitement limité ne devraient être traitées que pour la finalité qui a empêché leur effacement. Les méthodes visant à limiter le traitement de données à caractère personnel pourraient consister, entre autres, à déplacer les données sélectionnées vers un autre système de traitement, par exemple à des fins d'archivage, ou à rendre les données sélectionnées inaccessibles. Dans les fichiers automatisés, la limitation du traitement de données à caractère personnel devrait en principe être assurée par des moyens techniques; le fait que le traitement des données à caractère personnel est limité devrait être indiqué de manière à apparaître clairement dans le fichier. Cette rectification, cet effacement ou cette limitation de traitement devraient être communiqués aux destinataires auxquels les données ont été communiquées et aux autorités compétentes à l'origine des données inexactes. Les responsables du traitement devraient également cesser de diffuser ces données.

(36 *bis*) Lorsque le responsable du traitement refuse à une personne concernée le droit à l'information, le droit d'accès, de rectification et d'effacement ou le droit de limitation du traitement, la personne concernée devrait avoir le droit de demander à l'autorité de contrôle nationale de vérifier la licéité du traitement. La personne concernée devrait être informée de ce droit. Lorsque l'autorité de contrôle agit au nom de la personne concernée, elle devrait à tout le moins l'informer qu'elle a procédé à toutes les vérifications ou à tous les examens nécessaires. L'autorité de contrôle devrait également informer la personne concernée de son droit de former un recours juridictionnel.

(36 *bis bis*) Lorsque les données à caractère personnel sont traitées dans le cadre d'une enquête judiciaire ou d'une procédure pénale, l'exercice du droit à l'information, du droit d'accès, de rectification et d'effacement, et du droit de limitation du traitement peut être pratiqué conformément aux règles nationales de procédure pénale.

(37) Il y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. Il importe en particulier que le responsable du traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec la présente directive. Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités des traitements, ainsi que du risque que ceux-ci présentent pour les droits et libertés des personnes. Les mesures prises par le responsable du traitement devraient comprendre l'établissement et la mise en œuvre de garanties spécifiques destinées au traitement de données à caractère personnel relatives aux personnes vulnérables telles que les enfants.

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

(37 *ter*) Il convient de déterminer la probabilité et la gravité du risque en fonction de la nature, de la portée, du contexte et des finalités du traitement de données. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque élevé. On entend par risque élevé, un risque particulier de porter atteinte aux droits et aux libertés des personnes concernées.

(38) La protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel les concernant exige l'adoption de mesures techniques et organisationnelles appropriées, de sorte que les exigences de la présente directive soient respectées. La mise en œuvre de telles mesures ne peut dépendre uniquement de considérations économiques. Afin d'être en mesure de démontrer la conformité avec la présente directive, le responsable du traitement devrait adopter des règles internes et appliquer des mesures qui respectent en particulier les principes de la protection des données dès la conception et de la protection des données par défaut. Lorsque le responsable du traitement a procédé à une analyse d'impact relative à la protection des données en vertu de la présente directive, les résultats devraient être pris en compte lors de l'élaboration desdites mesures et procédures. Les mesures pourraient comprendre notamment le recours à la pseudonymisation dès que cela est possible. Le recours à la pseudonymisation aux fins de la présente directive peut servir d'outil susceptible de faciliter en particulier la libre circulation des données à caractère personnel dans l'Espace de liberté, de sécurité et de justice.

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

(39 *bis*) La réalisation de traitements par un sous-traitant devrait être régie par un acte juridique comprenant un contrat liant le sous-traitant au responsable du traitement et prévoyant notamment que le sous-traitant ne devrait agir que sur instruction du responsable du traitement. Le sous-traitant devrait tenir compte du principe de protection des données dès la conception et par défaut.

(40) Afin d'apporter la preuve qu'il se conforme à la présente directive, le responsable du traitement ou le sous-traitant devrait tenir des registres pour toutes les catégories d'activités de traitement de données à caractère personnel relevant de sa responsabilité. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à sa disposition sur demande pour qu'ils servent au contrôle de ces opérations de traitement. Le responsable du traitement ou le sous-traitant qui traite des données à caractère personnel dans des systèmes de traitement non automatisés devrait s'être doté des moyens effectifs de démontrer la licéité du traitement des données, de pratiquer l'autocontrôle et de garantir l'intégrité et la sécurité des données, tels que des journaux ou d'autres formes de registres.

(40 *bis*) Des journaux devraient être établis au moins pour les opérations effectuées sur des systèmes de traitement automatisé telles que la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion ou l'effacement. L'identification de la personne qui a consulté ou communiqué les données à caractère personnel devrait apparaître dans le journal et permettre d'établir les motifs justifiant les opérations de traitement. Les journaux devraient être utilisés uniquement à des fins de vérification de la licéité du traitement des données, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données et pour les besoins de procédures pénales. L'autocontrôle comprend aussi des procédures disciplinaires internes des autorités compétentes.

(40 *ter*) Lorsqu'un traitement est, du fait de sa nature, de sa portée ou de ses finalités, susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement devrait effectuer une analyse d'impact relative à la protection des données portant notamment sur les mesures, garanties et mécanismes envisagés pour assurer la protection des données à caractère personnel et apporter la preuve de la conformité avec la présente directive. Les analyses d'impact devraient porter sur les systèmes et processus pertinents des opérations de traitement de données à caractère personnel, et non sur des cas individuels.

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

(41 *bis*) Afin de préserver la sécurité et de prévenir tout traitement en violation de la présente directive, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le cryptage. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre au regard des risques liés au traitement et de la nature des données à caractère personnel à protéger. Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient d'apprécier les risques que présente le traitement de données, tels que la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, d'origine accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou moraux. Le responsable du traitement et le sous-traitant devraient veiller à ce que le traitement des données à caractère personnel ne soit pas effectué par des personnes non autorisées.

(42) Une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou moraux tels qu'une perte de maîtrise de leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social. En conséquence, dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite et que cette violation est susceptible d'engendrer un risque pour les droits et les libertés de la personne concernée, il convient qu'il en informe l'autorité de contrôle dans les meilleurs délais et, lorsque c'est possible, dans les 72 heures. Si ce délai ne peut être respecté, la notification devrait être assortie d'une explication concernant ce retard et les informations peuvent être fournies de manière échelonnée sans autre retard.

(43) Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, celle -ci devrait être avertie dans les meilleurs délais afin qu'elle puisse prendre les précautions qui s'imposent. La notification devrait décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne physique concernée afin d'atténuer les effets négatifs pouvant découler de ladite violation. Il convient que les notifications aux personnes physiques concernées soient effectuées aussi rapidement qu'il est raisonnablement possible, en coopération étroite avec l'autorité de contrôle et dans le respect des directives fournies par celle-ci ou par d'autres autorités compétentes. Par exemple, vu la nécessité d'atténuer un risque immédiat de dommage, il faudrait adresser rapidement une notification aux personnes concernées, mais la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données ou la survenance de violations similaires pourrait justifier un délai plus long. Lorsque le fait de retarder ou de limiter la communication à la personne physique concernée d'une violation des données à caractère personnel ne permet pas d'éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, d'éviter de nuire à la prévention et à la détection des infractions pénales, aux enquêtes et poursuites en la matière ou à l'exécution de sanctions pénales, de sauvegarder la sécurité publique ou nationale, ou de protéger les droits et libertés d'autrui, la communication pourrait, dans des circonstances exceptionnelles, être omise.

(44) Le responsable du traitement devrait désigner une personne qui l'aiderait à vérifier le respect, au niveau interne, des dispositions adoptées en vertu de la présente directive, sauf lorsqu'un État membre décide que des tribunaux et d'autres autorités judiciaires indépendantes sont dispensés dans l'exercice de leur fonction juridictionnelle. Cette personne peut être un membre du personnel du responsable du traitement ayant reçu une formation spéciale dans le domaine de la législation et des pratiques en matière de protection des données afin d'acquérir des connaissances spécialisées. Le niveau de connaissances spécialisées requis devrait être déterminé notamment en fonction du traitement des données effectué et de la protection exigée pour les données à caractère personnel traitées par le responsable du traitement. Cette personne peut exercer cette fonction à temps plein ou à temps partiel. Un délégué à la protection des données peut être désigné conjointement par plusieurs responsables du traitement, compte tenu de leur structure organisationnelle et de leur taille, par exemple en cas de partage des ressources au sein d'unités centrales. Cette personne peut également être désignée pour occuper différents postes au sein de la structure des responsables du traitement concernés. Elle devrait aider le responsable du traitement et les salariés traitant des données à caractère personnel en les informant et en les conseillant sur le respect des obligations leur incombant en matière de protection des données. Les délégués à la protection des données devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance dans le respect de la législation nationale.

(45) Les États membres devraient veiller à ce qu'un transfert vers un pays tiers ou à une organisation internationale n'ait lieu que s'il est nécessaire à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, et si le responsable du traitement dans le pays tiers ou dans l'organisation internationale est une autorité compétente au sens de la présente directive. Un transfert ne peut être effectué que par les autorités compétentes agissant en qualité de responsables du traitement, sauf dans le cas où les sous-traitants sont expressément chargés de procéder au transfert pour le compte des responsables du traitement. Un tel transfert peut avoir lieu lorsque la Commission a décidé que le pays tiers ou l'organisation internationale en question garantit un niveau adéquat de protection, ou lorsque des garanties appropriées ont été offertes ou que des dérogations pour des situations particulières s'appliquent. Lorsque des données à caractère personnel sont transférées de l'Union à des responsables du traitement, sous-traitants ou autres destinataires dans des pays tiers ou à des organisations internationales, il importe que le niveau de protection des personnes physiques garanti dans l'Union par la présente directive ne soit pas compromis, y compris en cas de transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale à des responsables du traitement ou sous-traitants dans le même pays tiers ou dans un pays tiers différent, ou à une autre organisation internationale.

(45 *bis*) Lorsque des données à caractère personnel sont transférées d'un État membre vers des pays tiers ou à des organisations internationales, un tel transfert ne devrait en principe avoir lieu qu'après que l'État membre auprès duquel les données ont été collectées a autorisé le transfert. Il est dans l'intérêt d'une coopération efficace en matière répressive que, lorsque le caractère immédiat de la menace pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre est tel qu'il rend impossible l'obtention d'une autorisation préalable en temps utile, l'autorité compétente puisse transférer les données à caractère personnel pertinentes vers le pays tiers concerné ou à l'organisation internationale concernée sans cette autorisation préalable. Les États membres devraient prévoir que les éventuelles conditions particulières applicables au transfert devraient être communiquées aux pays tiers et/ou aux organisations internationales. Les transferts ultérieurs de données à caractère personnel devraient être soumis à l'autorisation préalable de l'autorité compétente qui a procédé au transfert initial. Au moment de statuer sur une demande d'autorisation d'un transfert ultérieur, l'autorité compétente qui a procédé au transfert initial devrait prendre dûment en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction, les conditions particulières applicables et la finalité pour laquelle les données ont été transférées initialement, la nature et les conditions de l'exécution de la sanction pénale, et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel/laquelle les données à caractère personnel sont transférées ultérieurement. L'autorité compétente qui a effectué le transfert initial peut aussi assortir le transfert ultérieur de conditions particulières. Ces conditions particulières peuvent être décrites, par exemple, dans des codes de traitement.

(46) La Commission peut décider, avec effet dans l'ensemble de l'Union, que certains pays tiers, ou un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale offrent un niveau adéquat de protection des données, ce qui assurera une sécurité juridique et une uniformité dans l'ensemble de l'Union en ce qui concerne les pays tiers ou les organisations internationales qui sont réputés assurer un tel niveau de protection. Dans ce cas, les transferts de données à caractère personnel vers ces pays peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autorisation spécifique, à l'exception du cas où un autre État membre auprès duquel les données ont été collectées doit autoriser le transfert.

(47) Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait, dans son évaluation d'un pays tiers ou d'un territoire ou un secteur déterminé dans un pays tiers, prendre en considération la manière dont ce pays respecte l'État de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, notamment en ce qui concerne la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal. Lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision constatant le caractère adéquat de la protection, il y a lieu de se fonder sur des critères clairs et objectifs, comme les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti au sein de l'Union, en particulier quand les données sont traitées dans un ou plusieurs secteurs spécifiques. Plus particulièrement, le pays tiers devrait assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités européennes de protection des données, et les personnes concernées devraient se voir octroyer des droits effectifs et exécutoires ainsi que des possibilités effectives de recours administratif ou juridictionnel.

(47 *bis*) Outre les engagements internationaux pris par le pays tiers ou l'organisation internationale, la Commission devrait également tenir compte des obligations découlant de la participation du pays tiers ou de l'organisation internationale à des systèmes multilatéraux ou régionaux, notamment en matière de protection des données à caractère personnel, ainsi que de la mise en œuvre de ces obligations. Il y a lieu, en particulier, de prendre en considération l'adhésion du pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel. Aux fins de l'évaluation du niveau de protection assuré par des pays tiers ou des organisations internationales, la Commission devrait consulter le comité européen de la protection des données. La Commission devrait également tenir compte de toute décision qu'elle aurait prise constatant le caractère adéquat de la protection, conformément à l'article 41 du règlement (UE) XXX.

(47 *ter*) La Commission devrait surveiller le fonctionnement des décisions relatives au niveau de protection atteint par un pays tiers, ou un territoire ou un secteur déterminé dans un pays tiers, ou par une organisation internationale. Dans ses décisions constatant le caractère adéquat de la protection, la Commission devrait prévoir un mécanisme d'examen périodique de leur fonctionnement. Cet examen périodique devrait être effectué en consultation avec le pays tiers ou l'organisation internationale en question et tenir compte de l'ensemble des évolutions présentant un intérêt dans le pays tiers ou au sein de l'organisation internationale.

(48) La Commission devrait également pouvoir constater qu'un pays tiers, ou un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale n'assure plus un niveau adéquat de protection des données. Si tel est le cas, le transfert de données à caractère personnel vers ce pays tiers ou à cette organisation internationale devrait être interdit, à moins que les exigences énoncées à l'article 35 ou 36 soient respectées. Il y aurait lieu de prévoir des procédures de consultation entre la Commission et le pays tiers ou l'organisation internationale en question. La Commission devrait informer en temps utile le pays tiers ou l'organisation internationale des motifs de sa conclusion et engager des consultations en vue de remédier à la situation.

(49) Les transferts qui ne sont pas fondés sur une décision constatant le caractère adéquat de la protection ne devraient être autorisés que lorsque des garanties appropriées ont été offertes dans un instrument juridiquement contraignant assurant la protection des données à caractère personnel, ou lorsque le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et estime, au vu de cette évaluation, qu'il existe des garanties appropriées en matière de protection des données à caractère personnel. Il peut s'agir, par exemple, d'accords bilatéraux juridiquement contraignants que les États membres ont conclus et transposés dans leur ordre juridique et que les personnes concernées peuvent faire valoir, qui assurent le respect des exigences en matière de protection des données et des droits des personnes concernées, et notamment le droit de recours administratif ou juridictionnel effectif. Lorsqu'il évalue toutes les circonstances entourant le transfert de données, le responsable du traitement peut tenir compte des accords de coopération conclus entre Europol ou Eurojust et des pays tiers qui prévoient un échange de données à caractère personnel. Le responsable du traitement peut aussi prendre en compte le fait que le transfert de données à caractère personnel sera soumis à des obligations de confidentialité et au principe de spécificité, ce qui garantit que les données ne seront pas traitées à des fins autres que celles pour lesquelles elles ont été transférées. En outre, le responsable du traitement devrait prendre en compte le fait que les données à caractère personnel ne seront pas utilisées pour demander, prononcer ou mettre à exécution une condamnation à la peine de mort ou toute forme de traitement cruel et inhumain. Si ces conditions peuvent être considérées comme des garanties appropriées permettant le transfert de données, le responsable du traitement peut demander des garanties supplémentaires.

(49 *bis bis*) En l'absence de décision constatant le caractère adéquat de la protection ou de garanties appropriées, un transfert ou une catégorie de transferts ne peuvent être effectués que dans des situations particulières, s'ils sont nécessaires à la sauvegarde des intérêt vitaux de la personne concernée ou d'une autre personne ou à la sauvegarde des intérêts légitimes de la personne concernée lorsque la législation de l'État membre qui transfère les données à caractère personnel le prévoit, ou à la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers, ou, dans certains cas, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, ou, dans des cas particuliers, à la constatation, l'exercice ou la défense d'un droit en justice. Ces dérogations devraient être interprétées de manière restrictive et ne devraient pas permettre des transferts fréquents, massifs et structurels de données à caractère personnel ni des transferts à grande échelle de données, qui devraient être limités aux données strictement nécessaires. Ces transferts devraient être documentés et communiqués à l'autorité de contrôle, sur demande, afin qu'elle puisse en vérifier la licéité.

(49 *ter*) Les autorités compétentes des États membres appliquent les accords internationaux bilatéraux ou multilatéraux conclus avec des pays tiers qui sont en vigueur dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, aux fins d'échanger les informations nécessaires pour leur permettre d'accomplir les missions que leur confie la loi. En principe, ce processus se déroule moyennant, ou tout au moins avec, la coopération des autorités compétentes des pays tiers concernés, parfois même en l'absence d'un accord international bilatéral ou multilatéral. Cependant, dans certains cas particuliers, il se peut que les procédures normales exigeant de contacter l'autorité compétente dans le pays tiers soient inefficaces ou inappropriées, notamment parce que le transfert ne pourrait être effectué en temps opportun ou parce que l'autorité compétente dans le pays tiers ne respecte pas l'État de droit ou n'observe pas les règles et normes internationales dans le domaine des droits de l'homme si bien que les autorités compétentes des États membres pourraient décider de transférer les données à caractère personnel directement à des destinataires situés dans des pays tiers. C'est notamment le cas lorsqu'il est urgent de transférer des données à caractère personnel afin de sauver la vie d'une personne qui risque de devenir la victime d'une infraction pénale ou pour éviter la perpétration imminente d'un crime, y compris d'un acte de terrorisme. Même si ce transfert entre autorités compétentes et destinataires situés dans des pays tiers ne devrait intervenir que dans certains cas précis, la présente directive devrait prévoir les conditions qui régissent ces cas . Ces dispositions ne devraient pas être considérées comme constituant des dérogations aux accords internationaux bilatéraux ou multilatéraux en vigueur dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière. Ces règles devraient s'appliquer en complément des autres règles énoncées dans la directive, en particulier celles sur la licéité du traitement et celles du chapitre V.

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

(51) L'institution d'autorités de contrôle dans les États membres, exerçant leurs fonctions en toute indépendance, est un élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Il y a lieu que les autorités de contrôle surveillent l'application des dispositions adoptées en vertu de la présente directive et contribuent à ce que cette application soit cohérente dans l'ensemble de l'Union, afin de protéger les personnes physiques à l'égard du traitement des données à caractère personnel les concernant. À cet effet, les autorités de contrôle devraient coopérer entre elles et avec la Commission.

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

(53) Les États membres devraient avoir la possibilité d'instituer plusieurs autorités de contrôle en fonction de leur structure constitutionnelle, organisationnelle et administrative. Il convient que chaque autorité de contrôle soit dotée de tous les moyens financiers et humains ainsi que des locaux et des infrastructures nécessaires à la bonne exécution de ses missions, y compris celles qui sont liées à l'assistance mutuelle et à la coopération avec d'autres autorités de contrôle dans l'ensemble de l'Union. Chaque autorité de contrôle devrait disposer d'un budget annuel public propre, qui peut faire partie du budget national ou du budget d'une entité fédérée.

(53 *bis*) Les autorités de contrôle devraient être soumises à des mécanismes indépendants de contrôle ou de suivi de leur gestion financière, à condition que ce contrôle financier ne nuise pas à leur indépendance.

(54) Les conditions générales applicables au(x) membre(s) de l'autorité de contrôle devraient être fixées par la loi dans chaque État membre et prévoir notamment que ces membres sont nommés par le parlement ou le gouvernement ou le chef d'État de l'État membre, sur proposition du gouvernement ou d'un membre du gouvernement, ou du parlement ou de sa chambre, ou par un organisme indépendant chargé, par la législation de l'État membre, de procéder à la nomination selon une procédure transparente. Afin de garantir l'indépendance de l'autorité de contrôle, il convient que le membre ou les membres de celle-ci agissent avec intégrité, s'abstiennent de tout acte incompatible avec leurs fonctions et n'exercent, pendant la durée de leur mandat, aucune activité professionnelle incompatible, rémunérée ou non. Afin de garantir l'indépendance de l'autorité de contrôle, il convient que le personnel soit choisi par cette dernière, avec la possibilité qu'intervienne dans ce processus un organe indépendant qui en serait chargé par la législation de l'État membre.

(55) Bien que la présente directive s'applique également aux activités des juridictions nationales et autres autorités judiciaires, la compétence des autorités de contrôle ne devrait pas s'étendre au traitement de données à caractère personnel effectué par les tribunaux dans l'exercice de leur fonction juridictionnelle, afin de préserver l'indépendance des juges dans l'accomplissement de leurs missions judiciaires. Il convient que cette exception soit limitée aux activités judiciaires intervenant dans le cadre d'affaires portées devant les juridictions et qu'elle ne s'applique pas aux autres activités auxquelles les juges pourraient être associés en vertu de la législation nationale. Les États membres peuvent aussi prévoir que la compétence de l'autorité de contrôle ne peut pas s'étendre aux traitements de données à caractère personnel effectués par d'autres autorités judiciaires indépendantes dans l'exercice de leur fonction juridictionnelle, par exemple le parquet. En tout état de cause, le respect des règles de la présente directive par les juridictions et autres autorités judiciaires indépendantes devrait toujours faire l'objet d'un contrôle indépendant conformément à l'article 8, paragraphe 3, de la charte des droits fondamentaux de l'Union européenne.

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

(57) Afin d'assurer l'efficacité, la fiabilité et la cohérence du contrôle du respect et de l'application de la présente directive dans l'ensemble de l'Union conformément au traité tel qu'il a été interprété par la Cour de justice de l'Union européenne, les autorités de contrôle devraient avoir, dans chaque État membre, les mêmes missions et les mêmes pouvoirs effectifs, dont celui d'enquêter, d'adopter des mesures correctrices et d'émettre des avis consultatifs, qui constituent les moyens nécessaires à l'accomplissement de leurs missions. Cependant, leurs pouvoirs ne devraient pas interférer avec les règles spécifiques établies pour la procédure pénale, y compris pour les enquêtes et les poursuites concernant les infractions pénales, ni avec l'indépendance du pouvoir judiciaire. Sans préjudice des pouvoirs des autorités chargées des poursuites en vertu de la législation nationale, les autorités de contrôle devraient aussi avoir le pouvoir de porter les infractions à la présente directive à l'attention des autorités judiciaires et/ou d'ester en justice. Les pouvoirs des autorités de contrôle devraient être exercés en conformité avec les garanties procédurales appropriées prévues par le droit de l'Union et la législation des États membres, d'une manière impartiale et équitable et dans un délai raisonnable. Cela signifie que toute mesure devrait être appropriée, nécessaire et proportionnée en vue de garantir le respect de la présente directive, compte tenu des circonstances de l'espèce, respecter le droit de chacun à être entendu avant que soit prise toute mesure individuelle susceptible de l'affecter défavorablement et éviter les coûts superflus ainsi que les désagréments excessifs pour les personnes concernées. Les pouvoirs d'enquête en ce qui concerne l'accès aux installations devraient être exercés dans le respect des exigences spécifiques de la législation nationale, par exemple l'obligation d'obtenir une autorisation judiciaire préalable. Si une décision juridiquement contraignante est adoptée, elle devrait donner lieu à un contrôle juridictionnel dans l'État membre de l'autorité de contrôle qui l'a adoptée.

(58) Les autorités de contrôle devraient s'entraider et se prêter mutuellement assistance dans l'accomplissement de leurs missions afin d'assurer une application cohérente des dispositions adoptées en vertu de la présente directive.

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

(60) Toute personne concernée devrait avoir le droit d'introduire une réclamation auprès d'une autorité de contrôle unique et disposer d'un droit à un recours juridictionnel effectif conformément à l'article 47 de la charte des droits fondamentaux de l'Union européenne si elle estime que les droits que lui confèrent les dispositions adoptées en vertu de la présente directive ne sont pas respectés, si l'autorité de contrôle ne donne pas suite à sa réclamation, la refuse ou la rejette, en tout ou en partie, ou si elle n'agit pas alors qu'une action est nécessaire pour protéger les droits de la personne concernée. L'enquête faisant suite à une réclamation devrait être menée, sous contrôle juridictionnel, dans la mesure appropriée requise par l'affaire. L'autorité de contrôle compétente devrait informer la personne concernée de l'état d'avancement et de l'issue de la réclamation dans un délai raisonnable. Si l'affaire requiert un complément d'enquête ou une coordination avec une autre autorité de contrôle, des informations intermédiaires devraient être fournies à la personne concernée. Afin de faciliter l'introduction des réclamations, chaque autorité de contrôle devrait prendre des mesures telles que la fourniture d'un formulaire de réclamation qui peut être rempli également par voie électronique, sans que d'autres moyens de communication soient exclus.

(61) Toute personne physique ou morale devrait disposer d'un droit de recours juridictionnel effectif, devant la juridiction nationale compétente, contre une décision d'une autorité de contrôle qui produit des effets juridiques à son égard. Une telle décision concerne en particulier l'exercice, par l'autorité de contrôle, de pouvoirs d'enquête, d'adoption de mesures correctrices et d'autorisation ou le refus ou le rejet de réclamations. Toutefois, ce droit ne concerne pas d'autres mesures des autorités de contrôle qui ne sont pas juridiquement contraignantes, telles que les avis émis ou les conseils fournis par une autorité de contrôle. Les actions contre une autorité de contrôle devraient être intentées devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie et être menées conformément à la législation de l'État membre en question. Ces juridictions devraient disposer d'une pleine compétence, et notamment de celle d'examiner tous les éléments de fait et de droit relatifs au litige dont elles sont saisies.

(62) Lorsqu'une personne concernée estime que les droits que lui confère la présente directive ne sont pas respectés, elle devrait avoir le droit de mandater un organisme qui œuvre à la protection des droits et intérêts des personnes concernées dans le domaine de la protection des données à caractère personnel et qui est constitué conformément à la législation d'un État membre, pour qu'il introduise une réclamation en son nom auprès d'une autorité de contrôle et pour qu'il exerce le droit à un recours juridictionnel. Le droit de représentation des personnes concernées ne devrait pas porter atteinte à une législation procédurale nationale pouvant prévoir que les personnes concernées doivent être obligatoirement représentées devant les juridictions nationales par un avocat au sens de la directive 77/249/CEE.

(63) (…)

(64) Tout dommage qu'une personne pourrait subir du fait d'un traitement non conforme aux dispositions adoptées en vertu de la présente directive devrait être réparé par le responsable du traitement ou toute autre autorité compétente en vertu de la législation nationale. La notion de dommage devrait être interprétée au sens large, à la lumière de la jurisprudence de la Cour de justice de l'Union européenne, de façon à tenir pleinement compte des objectifs de la présente directive. Cela est sans préjudice de toute action en dommages-intérêts fondée sur une infraction à d'autres règles du droit de l'Union ou de la législation d'un État membre. Lorsqu'il est fait référence à un traitement illicite ou non conforme aux dispositions adoptées en vertu de la présente directive, cela concerne aussi un traitement non conforme aux actes d'exécution adoptés conformément à la présente directive. Les personnes concernées devraient recevoir une indemnisation complète et effective pour le dommage subi.

(65) Toute personne physique ou morale, soumise au droit privé ou au droit public, qui ne respecte pas la présente directive devrait faire l'objet de sanctions. Les États membres devraient veiller à ce que les sanctions soient effectives, proportionnées et dissuasives, et prendre toutes les mesures nécessaires à leur mise en œuvre.

(66) (…)

(67) Afin d'assurer des conditions uniformes d'exécution de la présente directive, il convient de conférer des compétences d'exécution à la Commission en ce qui concerne le niveau adéquat de protection offert par un pays tiers, ou un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale ainsi que la forme et les procédures de l'assistance mutuelle et les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle et entre les autorités de contrôle et le comité européen de la protection des données. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission.[7]

(68) Il convient d'avoir recours à la procédure d'examen pour l'adoption d'actes d'exécution en ce qui concerne le niveau adéquat de protection atteint par un pays tiers ou un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale ainsi que la forme et les procédures de l'assistance mutuelle et les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle et entre les autorités de contrôle et le comité européen de la protection des données, étant donné que ces actes sont de portée générale.

(69) La Commission devrait adopter des actes d'exécution immédiatement applicables lorsque, dans des cas dûment justifiés liés à un pays tiers, ou un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale, qui n'assure plus un niveau adéquat de protection, des raisons d'urgence impérieuses le requièrent.

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

(70) Étant donné que les objectifs de la présente directive, à savoir protéger les libertés et les droits fondamentaux des personnes concernées, et en particulier leur droit à la protection des données personnelles, et garantir le libre échange de ces dernières par les autorités compétentes au sein de l'Union, ne peuvent pas être atteints de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets de l'action, être mieux atteints au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs. Les États membres peuvent prévoir des normes plus strictes que celles établies par la présente directive.

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

(72) Les dispositions particulières des actes de l'Union adoptés dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière avant la date d'adoption de la présente directive qui régissent le traitement de données à caractère personnel entre États membres ou l'accès d'autorités désignées des États membres aux systèmes d'information créés en vertu des traités devraient demeurent inchangées, notamment, par exemple, les dispositions particulières relatives à la protection des données à caractère personnel appliquées en vertu de la décision 2008/615/JAI[8] ou l'article 23 de la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (2000/C 197/01).[9] Étant donné que l'article 8 de la charte et l'article 16 du TFUE exigent que le droit fondamental à la protection des données à caractère personnel soit garanti de manière homogène dans l'ensemble de l'Union, la Commission devrait évaluer la situation en ce qui concerne la relation entre la présente directive et les actes adoptés avant la date de son adoption qui régissent le traitement des données à caractère personnel entre États membres ou l'accès d'autorités désignées des États membres aux systèmes d'information créés en vertu des traités, afin d'apprécier la nécessité de mettre ces dispositions particulières en conformité avec la présente directive. Le cas échéant, la Commission devrait faire des propositions en vue d'assurer la cohérence des règles juridiques relatives au traitement des données à caractère personnel.

---

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

9 Acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne, JO C 197 du 12.7.2000, p. 1.

(73) Afin d'assurer une protection exhaustive et cohérente des données à caractère personnel dans l'Union, il convient que les accords internationaux conclus par les États membres avant l'entrée en vigueur de la présente directive et qui sont conformes aux dispositions pertinentes du droit de l'Union applicables avant l'entrée en vigueur de la présente directive, restent en vigueur jusqu'à ce qu'ils soient modifiés, remplacés ou révoqués.

(73 *bis*) Les États membres devraient disposer d'un délai de deux ans maximum à compter de l'entrée en vigueur pour mettre en œuvre la présente directive. Les traitements déjà en cours à la date d'entrée en vigueur de la présente directive devraient être mis en conformité avec celle-ci dans un délai de deux ans après son entrée en vigueur. Toutefois, lorsque ces traitements ont lieu en conformité avec le droit de l'Union applicable avant l'entrée en vigueur de la présente directive, les exigences prévues par celle-ci concernant la consultation préalable de l'autorité de contrôle ne devraient pas s'appliquer aux traitements déjà en cours avant l'entrée en vigueur de la présente directive, étant donné qu'il convient de satisfaire à ces exigences, de par leur nature même, avant le traitement. Lorsque les États membres recourent au délai de mise en œuvre plus long, venant à expiration sept ans après la date d'entrée en vigueur de la présente directive, pour se conformer aux obligations en matière de journalisation pour les systèmes de traitement automatisé mis en place avant l'entrée en vigueur de la présente directive, le responsable du traitement ou le sous-traitant devrait s'être doté des moyens effectifs de démontrer la licéité du traitement des données, de pratiquer l'autocontrôle et de garantir l'intégrité et la sécurité des données, tels que des journaux ou d'autres formes de registres.

(74) La présente directive s'applique sans préjudice des dispositions relatives à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, et la pédopornographie qui figurent dans la directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011[10].

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

(75) Conformément à l'article 6 *bis* du protocole sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Royaume-Uni et l'Irlande ne sont pas liés par les règles fixées dans la présente directive concernant le traitement de données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne, lorsque le Royaume-Uni ou l'Irlande n'est pas lié par les règles qui régissent des formes de coopération judiciaire en matière pénale ou de coopération policière dans le cadre desquelles les dispositions fixées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne doivent être respectées.

(76) Conformément aux articles 2 et 2 *bis* du protocole sur la position du Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark n'est pas lié par les règles fixées dans la présente directive ni soumis à leur application, lorsqu'elles concernent le traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne. Étant donné que la présente directive développe l'acquis de Schengen, en vertu du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne, le Danemark décidera, conformément à l'article 4 dudit protocole, dans un délai de six mois après l'adoption de la présente directive, s'il transposera celle-ci dans son droit national.

(77) En ce qui concerne l'Islande et la Norvège, la présente directive constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[11].

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

(78) En ce qui concerne la Suisse, la présente directive constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[12].

(79) En ce qui concerne le Liechtenstein, la présente directive constitue un développement des dispositions de l'acquis de Schengen au sens du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[13].

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

(81) Conformément à la déclaration politique commune du 28 septembre 2011 des États membres et de la Commission sur les documents explicatifs[14], les États membres se sont engagés à joindre à la notification de leurs mesures de transposition, dans les cas où cela se justifie, un ou plusieurs documents expliquant le lien entre les éléments d'une directive et les parties correspondantes des instruments nationaux de transposition. En ce qui concerne la présente directive, le législateur estime que la transmission de ces documents est justifiée.

---

12 JO L 53 du 27.2.2008, p. 52.
13 JO L 160 du 18.6.2011, p. 21.
14 JO C 369 du 17.12.2011, p. 14.

(82) La présente directive ne saurait empêcher les États membres de mettre en œuvre l'exercice des droits des personnes concernées en matière d'information, d'accès, de rectification, d'effacement et de limitation du traitement de leurs données à caractère personnel dans le cadre de poursuites pénales, et les éventuelles limitations de ces droits, dans leur législation nationale en matière de procédure pénale,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I
DISPOSITIONS GÉNÉRALES

Article premier
Objet et objectifs

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

1 *bis*. La présente directive n'empêche pas les États membres de prévoir des garanties plus strictes que celles établies en vertu de la présente directive pour la protection des droits et des libertés des personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes.

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

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

   b) veillent à ce que l'échange de données à caractère personnel par les autorités compétentes au sein de l'Union, lorsque cet échange est requis en vertu du droit de l'Union ou de la législation nationale, ne soit ni limité ni interdit pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Article 2
Champ d'application

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

2. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

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

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

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

Article 3
Définitions

Aux fins de la présente directive, on entend par:

1) "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 identifiant, par exemple un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

2) (…)

3) "traitement", toute opération ou tout 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 structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation, l'effacement ou la destruction;

4) "limitation du traitement", le marquage de données à caractère personnel enregistrées, en vue de limiter leur traitement futur;

4 *bis*) "pseudonymisation", le traitement de données à caractère personnel de telle façon qu'elles ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable;

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

6) "responsable du traitement", l'autorité compétente qui, seule 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 déterminés par le droit de l'Union ou la législation d'un État membre, le responsable du traitement peut être désigné, ou les critères spécifiques applicables pour le désigner peuvent être fixés, par le droit de l'Union ou la législation d'un État membre;

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

8) "destinataire", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière conformément à la législation nationale ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement;

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

10) "données génétiques", toutes les données à caractère personnel liées aux caractéristiques génétiques d'une personne physique qui sont héréditaires ou ont été acquises, et qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne, résultant en particulier d'une analyse d'un échantillon biologique de la personne en question;

11) "données biométriques", toute donnée à caractère personnel résultant d'un traitement technique spécifique, relative aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permet ou confirme son identification unique, telles que des images faciales ou des données dactyloscopiques;

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

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

13) (…)

14) "autorité compétente",

a) toute autorité publique compétente à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ou

b) tout autre organisme ou entité à qui la législation nationale confie l'exercice de l'autorité publique et de prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

15) "autorité de contrôle", une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 39;

16) "organisation internationale", une organisation internationale et les organismes de droit international public qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou dont la création est fondée sur un tel accord.

CHAPITRE II
PRINCIPES

Article 4

Principes relatifs au traitement des données à caractère personnel

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

   a) traitées de manière licite et loyale;

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

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

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

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

   f) (…)

   f *ter*) traitées de façon à garantir une sécurité appropriée des données, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

2. Le traitement des données, par le même ou un autre responsable du traitement, pour des finalités énoncées à l'article 1er, paragraphe 1, autres que celles pour lesquelles les données ont été collectées est autorisé à condition que:

   a) le responsable du traitement soit autorisé à traiter ces données à caractère personnel pour une telle finalité conformément au droit de l'Union ou à la législation d'un État membre, et

b) le traitement soit nécessaire et proportionné à cette autre finalité conformément au droit de l'Union ou à la législation d'un État membre.

3. Le traitement des données par le même ou un autre responsable du traitement peut inclure l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques pour les finalités énoncées à l'article 1er, paragraphe 1, sous réserve de garanties appropriées concernant les droits et libertés de la personne concernée.

4. Le responsable du traitement est responsable du respect des dispositions figurant aux paragraphes 1, 2 et 3 et est en mesure de démontrer que ces dispositions sont respectées.

Article 4 ter

Délais de conservation et d'examen

Les États membres prévoient que des délais appropriés sont fixés pour effacer les données à caractère personnel ou vérifier régulièrement s'il est nécessaire de conserver les données. Des règles procédurales permettent d'assurer le respect de ces délais.

Article 5

Distinction entre différentes catégories de personnes concernées

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

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

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

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

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

e) (…)

Article 6

Différenciation des données à caractère personnel et vérification de la qualité des données

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

2. Les États membres prévoient que les autorités compétentes prennent toutes les mesures raisonnables pour assurer que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour ne soient pas transmises ou mises à disposition. À cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition. Dans la mesure du possible, lors de toute transmission de données à caractère personnel, les informations nécessaires sont jointes aux données, afin que l'autorité compétente destinataire puisse juger de l'exactitude, de l'exhaustivité, et de la fiabilité desdites données à caractère personnel, et vérifier qu'elles sont encore d'actualité.

3. S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données ont été transmises illicitement, le destinataire en est informé immédiatement. Dans ce cas, les données à caractère personnel doivent être rectifiées ou effacées ou leur transmission doit être limitée en application de l'article 15.

Article 7

Licéité du traitement

1. Les États membres prévoient que le traitement des données à caractère personnel n'est licite que si, et dans la mesure où, il est nécessaire à l'exécution d'une mission par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1, et fondé sur le droit de l'Union ou la législation d'un État membre.

   a) (…)

   b) (…)

   c) (…)

   d) (…)

1 *bis*. La législation d'un État membre qui régit le traitement des données à caractère personnel relevant du champ d'application de la présente directive précise au moins les objectifs, les données à caractère personnel qui feront l'objet d'un traitement et les finalités du traitement.

Article 7 bis

Conditions spécifiques applicables au traitement

1. Des données à caractère personnel collectées par des autorités compétentes pour les finalités énoncées à l'article 1er, paragraphe 1, ne peuvent être traitées à des fins autres que celles énoncées à l'article 1er, paragraphe 1, que lorsqu'un tel traitement est autorisé par le droit de l'Union ou la législation d'un État membre. Dans ces cas, le règlement (UE) ..../XXX s'applique à ce traitement, à moins que le traitement soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.

1 *bis*. Lorsque les autorités compétentes sont chargées par la législation d'un État membre d'exécuter des missions pour des finalités autres que celles énoncées à l'article 1er, paragraphe 1, le règlement (UE) ..../XXX s'applique au traitement effectué à de telles fins, y compris à des fins d'archivage dans l'intérêt public, à des fins statistiques, scientifiques ou historiques, à moins que le traitement soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.

1 *ter*. Les États membres prévoient que, lorsque le droit de l'Union ou la législation d'un État membre applicable à l'autorité compétente qui transmet les données soumet le traitement de données à caractère personnel à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces conditions et de l'obligation de les respecter.

2. Les États membres prévoient que l'autorité compétente qui transmet les données n'applique pas aux destinataires dans les autres États membres ou aux institutions, organes et organismes établis en vertu des chapitres IV et V du titre V du traité sur le fonctionnement de l'Union européenne des conditions visées au paragraphe 1 *ter* différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État membre dans lequel ladite autorité est établie.

Article 8

Traitement portant sur des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques permettant d'identifier une personne de manière univoque ou des données concernant la santé ou la vie et l'orientation sexuelles sont autorisés uniquement en cas de nécessité absolue, et sous réserve de garanties appropriées applicables aux droits et aux libertés de la personne concernée, et uniquement:

   a) lorsqu'ils sont autorisés par le droit de l'Union ou la législation d'un État membre; ou

   b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne; ou

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

2. (…)

Article 9

Décision individuelle automatisée

1. Les États membres prévoient que toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative est interdite, à moins qu'elle ne soit autorisée par le droit de l'Union ou la législation d'un État membre auquel le responsable du traitement est soumis et qui comporte des garanties appropriées applicables aux droits et aux libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement.

2. Les décisions visées au paragraphe 1 du présent article ne sauraient être fondées sur les catégories particulières de données à caractère personnel visées à l'article 8, à moins que des mesures appropriées garantissant la sauvegarde des droits et des libertés ainsi que des intérêts légitimes de la personne concernée ne soient en place.

2 *ter*. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base de catégories particulières de données à caractère personnel visées à l'article 8 est interdit, conformément au droit de l'Union.

CHAPITRE III
DROITS DE LA PERSONNE CONCERNÉE

Article 10

Communication et modalités de l'exercice des droits de la personne concernée

1. (…)

2. Les États membres prévoient que le responsable du traitement prend des mesures raisonnables pour fournir toute information visée à l'article 10 *bis*, ainsi que pour procéder à toute communication au titre de l'article 9, des articles 12 à 17 et de l'article 29 en ce qui concerne le traitement des données à caractère personnel de la personne concernée d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par tout moyen approprié, y compris par voie électronique. De manière générale, le responsable du traitement fournit les informations sous la même forme que la demande.

3. Les États membres prévoient que le responsable du traitement facilite l'exercice des droits conférés à la personne concernée en vertu de l'article 9 et des articles 12 à 17.

4. Les États membres prévoient que le responsable du traitement informe par écrit, dans les meilleurs délais, la personne concernée des suites données sa demande.

5. Les États membres prévoient qu'aucun paiement n'est exigé pour fournir les informations visées à l'article 10 *bis* et pour procéder à toute communication et prendre toute mesure au titre de l'article 9, des articles 12 à 17 et de l'article 29. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations pour procéder à la communication ou pour prendre les mesures demandées, ou refuser de donner suite à ces demandes. Dans ces cas, il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande .

5 *bis*. Lorsque le responsable du traitement a des doutes fondés quant à l'identité de la personne physique présentant la demande visée à l'article 12 ou 15, il peut demander que lui soient fournis des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

Article 10 bis

Informations mises à disposition de la personne concernée

1. Les États membres prévoient que le responsable du traitement met à la disposition de la personne concernée au moins les informations suivantes:

   a) l'identité et les coordonnées du responsable du traitement; le responsable du traitement inclut en outre les coordonnées du délégué à la protection des données, s'il en a désigné un;

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

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

   d) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel relatives à la personne concernée, la rectification ou l'effacement de celles-ci, ou la limitation de leur traitement.

2. Les États membres prévoient, par voie législative, que le responsable du traitement fournit à la personne concernée, dans des cas particuliers, les informations suivantes, en plus de celles visées au paragraphe 1, afin de lui permettre d'exercer ses droits:

   a) la base juridique du traitement,

   b) la durée pendant laquelle les données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

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

   d) au besoin, des informations complémentaires, en particulier lorsque les données sont collectées à l'insu de la personne concernée.

3. Les États membres peuvent adopter des mesures législatives visant à retarder ou limiter la fourniture des informations à communiquer à la personne concernée en application du paragraphe 2, ou à ne pas fournir de ces informations, dès lors et aussi longtemps qu'une mesure de cette nature est nécessaire et proportionnée dans une société démocratique, eu égard aux droits fondamentaux et aux intérêts légitimes de la personne concernée:

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

   b) pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

   c) pour protéger la sécurité publique;

   d) pour protéger la sécurité nationale;

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

4. Les États membres peuvent adopter des mesures législatives afin de déterminer des catégories de traitements de données susceptibles de faire l'objet, dans leur intégralité ou en partie, des dérogations prévues au paragraphe 3.

Article 11

(…)

Article 12

Droit d'accès de la personne concernée

1. Sous réserve de l'article 13, les États membres prévoient que la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations suivantes:

   a) les finalités du traitement ainsi que sa base juridique;

   b) les catégories de données à caractère personnel concernées;

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

   d) lorsque cela est possible, la durée pendant laquelle il est envisagé que les données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

   e) l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de ces données, ou la limitation de leur traitement ;

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

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

2. (…)

Article 13

Limitations du droit d'accès

1. Les États membres peuvent adopter des mesures législatives limitant, entièrement ou partiellement, le droit d'accès de la personne concernée, dès lors que, pour la période envisagée, une telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, eu égard aux droits fondamentaux et aux intérêts légitimes de la personne concernée:

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

   b) pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

   c) pour protéger la sécurité publique;

   d) pour protéger la sécurité nationale;

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

2. Les États membres peuvent adopter des mesures législatives afin de déterminer des catégories de traitements de données susceptibles de faire l'objet, dans leur intégralité ou en partie, des dérogations prévues au paragraphe 1.

3. Dans les cas visés aux paragraphes 1 et 2, les États membres prévoient que le responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, de tout refus ou de toute limitation de l'accès aux données, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au paragraphe 1. Les États membres prévoient que le responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.

4. Les États membres veillent à ce que le responsable du traitement conserve une trace documentaire des motifs de fait ou de droit fondant la décision. Ces informations sont mises à la disposition des autorités de contrôle.

Article 14

(...)

Article 15

Droit de rectification, d'effacement et de limitation du traitement

1. Les États membres prévoient le droit pour la personne concernée d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Eu égard à la finalité du traitement concerné, les États membres prévoient que la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris par la fourniture à cet effet d'une déclaration complémentaire.

1 *bis*. Les États membres prévoient que le responsable du traitement a l'obligation d'effacer dans les meilleurs délais les données à caractère personnel et que la personne concernée a le droit d'obtenir du responsable du traitement l'effacement dans les meilleurs délais de données à caractère personnel la concernant lorsque le traitement n'est pas conforme aux dispositions adoptées en vertu des articles 4, 7 et 8 de la présente directive ou lorsque les données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.

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

a) lorsque l'exactitude des données est contestée par la personne concernée et qu'il ne peut être déterminé si les données sont exactes ou non; ou

b) si les données doivent être conservées à des fins probatoires.

1 *quater*. Lorsque le traitement des données à caractère personnel est limité en vertu du paragraphe 1 *ter*, point a), le responsable du traitement informe la personne concernée avant de lever la limitation frappant le traitement.

2. Les États membres prévoient que le responsable du traitement informe la personne concernée par écrit de tout refus de rectifier ou d'effacer des données ou d'en limiter le traitement, ainsi que des motifs du refus. Les États membres peuvent adopter des mesures législatives limitant, entièrement ou partiellement, l'obligation de fournir ces informations, dès lors qu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique eu égard aux droits fondamentaux et aux intérêts légitimes de la personne concernée:

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

b) pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

c) pour protéger la sécurité publique;

d) pour protéger la sécurité nationale;

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

Les États membres prévoient que le responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.

2 *ter*. Les États membres prévoient que le responsable du traitement communique la rectification des données à caractère personnel inexactes à l'autorité compétente dont proviennent les données à caractère personnel inexactes.

3. Les États membres prévoient que, dans les cas visés aux paragraphes 1, 1 *bis*, 1 *ter* et 1 *quater*, le responsable du traitement adresse une notification aux destinataires et que ceux-ci rectifient ou effacent les données à caractère personnel relevant de leur responsabilité ou en limitent le traitement.

Article 15 bis

Exercice des droits de la personne concernée et vérification par l'autorité de contrôle

1. Dans les cas visés à l'article 10 *bis*, paragraphe 3, à l'article 13, paragraphe 3, et à l'article 15, paragraphe 2, les États membres adoptent des mesures afin que les droits de la personne concernée puissent également être exercés par l'intermédiaire de l'autorité de contrôle compétente.

1 *bis*. Les États membres prévoient que le responsable du traitement informe la personne concernée de la possibilité qu'elle a d'exercer ses droits par l'intermédiaire de l'autorité de contrôle en application du paragraphe 1.

2. Lorsque les droits visés au paragraphe 1 sont exercés, l'autorité de contrôle informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. L'autorité de contrôle informe également la personne concernée de son droit de former un recours juridictionnel.

Article 16

(...)

Article 17

Droits des personnes concernées lors des enquêtes judiciaires et des procédures pénales

Les États membres peuvent prévoir que les droits visés aux articles 10 *bis*, 12 et 15 sont exercés conformément à la législation nationale lorsque les données à caractère personnel figurent dans une décision judiciaire ou un casier ou dossier judiciaire faisant l'objet d'un traitement lors d'une enquête judiciaire ou d'une procédure pénale.

CHAPITRE IV
RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT

SECTION 1
OBLIGATIONS GÉNÉRALES

Article 18

Obligations incombant au responsable du traitement

1. Les États membres prévoient que, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement des données à caractère personnel est effectué dans le respect de la présente directive. Ces mesures sont réexaminées et actualisées, si nécessaire.

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

2. (…)

3. (…)

Article 19

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

1. Les États membres prévoient que, compte tenu de l'état des connaissances et des coûts de la mise en œuvre et prenant en considération la nature, la portée, le contexte et les finalités du traitement, ainsi que les risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant lors de la détermination des moyens du traitement que lors du traitement proprement dit, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à donner effet aux principes de la protection des données, par exemple la minimisation des données, de façon effective et de manière à ce que le traitement comporte les garanties nécessaires, afin de répondre aux exigences de la présente directive et de protéger les droits des personnes concernées.

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

Article 20

Responsables conjoints du traitement

1. Les États membres prévoient que, lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement de données à caractère personnel, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives afin de se conformer aux exigences de la présente directive, en ce qui concerne notamment l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées à l'article 10 *bis*, par voie d'accord, sauf si et dans la mesure où leurs obligations respectives sont définies par le droit de l'Union ou la législation de l'État membre applicable aux responsables du traitement. Le point de contact pour les personnes concernées est désigné dans l'accord. Les États membres peuvent préciser lequel des responsables conjoints peut servir de point de contact unique pour que les personnes concernées puissent exercer leurs droits.

1 *bis*. Indépendamment des termes de l'accord visé au paragraphe 1, les États membres peuvent prévoir que la personne concernée peut exercer les droits que lui confèrent les dispositions adoptées en vertu de la présente directive à l'égard de et contre chacun des responsables du traitement.

Article 21

Sous-traitant

1. Les États membres prévoient que le responsable du traitement, lorsque une opération de traitement doit être effectuée pour son compte, fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes de mise en œuvre des mesures techniques et organisationnelles appropriées, de manière à ce que le traitement soit conforme aux exigences de la présente directive et garantisse la protection des droits de la personne concernée.

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

2. Les États membres prévoient que la réalisation d'un traitement par un sous-traitant est régie par un contrat ou un autre acte juridique au titre du droit de l'Union ou de la législation d'un État membre, liant le sous-traitant au responsable du traitement, définissant l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, les obligations et les droits du responsable du traitement et prévoyant notamment que le sous-traitant:

a) n'agit que sur instruction du responsable du traitement;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation statutaire appropriée de confidentialité;

c) aide le responsable du traitement, par les moyens appropriés, à veiller au respect des dispositions relatives aux droits de la personne concernée;

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

e) met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect des obligations prévues par le présent article;

f) respecte les conditions visées aux paragraphes 1 *bis* et 2 pour recruter un autre sous-traitant.

2 *bis*. Le contrat ou l'autre acte juridique visé au paragraphe 2 est écrit, y compris en format électronique.

3. Si, en violation de la présente directive, un sous-traitant détermine les finalités et les moyens du traitement de données à caractère personnel, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement.

Article 22

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

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

Article 23

Registre des activités de traitement

1. Les États membres prévoient que chaque responsable du traitement tient un registre de toutes les catégories d'activités de traitement de données à caractère personnel mises en œuvre sous sa responsabilité. Ce registre comporte les informations suivantes:

   a) le nom et les coordonnées du responsable du traitement, de tout responsable conjoint du traitement et du délégué à la protection des données;

   b) les finalités du traitement;

   c) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires établis dans des pays tiers;

   c *bis*) une description des catégories de personnes concernées et des catégories de données à caractère personnel;

   c *ter*) le cas échéant, le recours au profilage;

   d) le cas échéant, les catégories de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale;

   d *bis*) une indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données sont destinées;

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

   f) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 27, paragraphe 1.

2. (…)

2 *bis*. Les États membres prévoient que chaque sous-traitant tient un registre de toutes les catégories de traitements de données à caractère personnel effectués pour le compte du responsable du traitement, comprenant:

a) le nom et les coordonnées du ou des sous-traitants, de chaque responsable du traitement pour le compte duquel le sous-traitant agit et du délégué à la protection des données éventuellement désigné;

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

c) le cas échéant, les transferts de données vers un pays tiers ou à une organisation internationale, y compris leur identification respective, lorsqu'il en est expressément chargé par le responsable du traitement;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 27, paragraphe 1.

2 *ter*. Les registres visés aux paragraphes 1 et 2 *bis* se présentent sous une forme écrite, y compris électronique.

3. Sur demande, le responsable du traitement et le sous-traitant mettent le registre à la disposition de l'autorité de contrôle.

Article 24

Journalisation

1. Les États membres veillent à ce que des journaux soient établis au moins pour les opérations de traitement ci-après dans des systèmes de traitement automatisé: la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion ou l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données.

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

2 *bis*. Le responsable du traitement et le sous-traitant mettent les journaux à la disposition de l'autorité de contrôle, sur demande.

Article 25

Coopération avec l'autorité de contrôle

1. Les États membres prévoient que le responsable du traitement et le sous-traitant coopèrent, sur demande, avec l'autorité de contrôle dans l'exercice de ses fonctions.

2. (…)

Article 25 bis

Analyse d'impact relative à la protection des données

1. Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, les États membres prévoient que le responsable du traitement effectue avant le traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

2. L'analyse contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, les mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve de la conformité avec les dispositions de la présente directive, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées.

Article 26

Consultation préalable de l'autorité de contrôle

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

   a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 25 *bis*, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; ou

   b) lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.

1 *bis*. Les États membres veillent à ce que l'autorité de contrôle soit consultée dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative qui se rapporte au traitement de données à caractère personnel.

2. Les États membres prévoient que l'autorité de contrôle peut établir une liste des opérations de traitement devant faire l'objet d'une consultation préalable conformément au paragraphe 1.

2 *bis*. Les États membres prévoient que le responsable du traitement fournit à l'autorité de contrôle l'analyse d'impact relative à la protection des données conformément à l'article 25 *bis* et, sur demande, toute autre information afin de permettre à l'autorité de contrôle d'apprécier la conformité du traitement et, en particulier, les risques pour la protection des données à caractère personnel de la personne concernée et les garanties qui s'y rapportent.

3. Les États membres prévoient que, lorsque l'autorité de contrôle est d'avis que le traitement prévu, visé au paragraphe 1, ne serait pas conforme aux dispositions adoptées en vertu de la présente directive, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, elle fournit par écrit, dans un délai maximum de six semaines suivant la demande de consultation, des conseils au responsable du traitement de données, et le cas échéant au sous-traitant, et peut faire usage des pouvoirs visés à l'article 46. Ce délai peut être prolongé d'un mois, compte tenu de la complexité du traitement prévu. En cas de prolongation du délai, le responsable du traitement et, le cas échéant, le sous-traitant sont informés dans un délai d'un mois à compter de la réception de la demande, y compris des raisons du report.

SECTION 2
SÉCURITÉ DES DONNÉES

Article 27

Sécurité du traitement

1. Les États membres prévoient que, compte tenu de l'état des connaissances et des coûts de la mise en œuvre et prenant en considération la nature, la portée, le contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données visé à l'article 8.

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

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

   b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);

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

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

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

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

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

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

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

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

3. (…)

Article 28

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

1. Les États membres prévoient qu'en cas de violation de données à caractère personnel, le responsable du traitement en adresse notification à l'autorité de contrôle dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins qu'il soit peu probable que la violation en question engendre des risques pour les droits et les libertés d'une personne physique. Lorsqu'elle a lieu après ce délai de 72 heures, la notification comporte une motivation.

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

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

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

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

c) (…)

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

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

3 *bis*. Si et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée dans les meilleurs délais.

4. Les États membres prévoient que le responsable du traitement conserve une trace documentaire de toute violation de données à caractère personnel visée au paragraphe 1, en indiquant son contexte, ses effets et les mesures prises pour y remédier. La documentation constituée doit permettre à l'autorité de contrôle de vérifier le respect des dispositions du présent article.

4 *bis*. Les États membres prévoient que, lorsque la violation de données porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre État membre ou à celui-ci, les informations visées au paragraphe 3 sont communiquées au responsable du traitement de cet État membre dans les meilleurs délais.

5. (…)

6. (…)

Article 29

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

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

2. La communication à la personne concernée visée au paragraphe 1 décrit en des termes clairs et simples la nature de la violation de données à caractère personnel et contient au moins les informations et les recommandations prévues à l'article 28, paragraphe 3, points b), d) et e).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si:

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

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

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

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

4. La communication à la personne concernée visée au paragraphe 1 peut être retardée, limitée ou omise, sous réserve des conditions et pour les motifs visés à l'article 10 *bis*, paragraphe 3.

SECTION 3
DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Article 30

Désignation du délégué à la protection des données

1. Les États membres prévoient que le responsable du traitement désigne un délégué à la protection des données. Les États membres peuvent dispenser les tribunaux et d'autres autorités judiciaires indépendantes de cette obligation dans l'exercice de leur fonction juridictionnelle.

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

3. Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes, compte tenu de leur structure organisationnelle et de leur taille.

3 *bis*. Les États membres prévoient que le responsable du traitement publie les coordonnées du délégué à la protection des données et les communique à l'autorité de contrôle.

Article 31

Fonction du délégué à la protection des données

1. Les États membres prévoient que le responsable du traitement veille à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

2. Le responsable du traitement aide le délégué à la protection des données à exercer les missions visées à l'article 32 en fournissant les ressources nécessaires à l'exécution de ces missions ainsi que l'accès aux données à caractère personnel et aux traitements, et lui permettant d'entretenir ses connaissances spécialisées.

Article 32

Missions du délégué à la protection des données

Les États membres prévoient que le responsable du traitement confie au délégué à la protection des données au moins les missions suivantes:

a) informer et conseiller le responsable du traitement et les salariés traitant des données à caractère personnel sur les obligations qui leur incombent en vertu de la présente directive et d'autres dispositions de l'Union ou d'un État membre en matière de protection des données;

b) contrôler la conformité avec la présente directive, avec d'autres dispositions de l'Union ou d'un État membre en matière de protection des données et avec les règles internes du responsable du traitement en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;

c) (…)

d) (…)

e) (…)

f) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci conformément à l'article 25 *bis*;

g) coopérer avec l'autorité de contrôle;

h) faire office de point de contact pour l'autorité de contrôle sur les questions liées au traitement de données à caractère personnel, y compris la consultation préalable visée à l'article 26, et consulter celle-ci, le cas échéant, sur tout autre sujet.

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

Article 33

Principes généraux applicables aux transferts de données à caractère personnel

1. Les États membres prévoient qu'un transfert, par des autorités compétentes, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après leur transfert vers un pays tiers ou à une organisation internationale, y compris des transferts ultérieurs vers un autre pays tiers ou à une autre organisation internationale, ne peut avoir lieu, sous réserve de la conformité avec les dispositions nationales adoptées en application d'autres dispositions de la présente directive, que si les conditions définies dans le présent chapitre sont respectées, à savoir:

   a) le transfert est nécessaire aux fins énoncées à l'article 1er, paragraphe 1; et

   b) (…);

   c) les données sont transférées à un responsable du traitement dans un pays tiers ou à une organisation internationale qui est une autorité compétente aux fins visées à l'article 1er, paragraphe 1; et

   d) en cas de transmission ou de mise à disposition de données à caractère personnel provenant d'un autre État membre, celui-ci a préalablement autorisé ce transfert en conformité avec sa législation nationale; et

   e) la Commission a décidé, conformément à l'article 34, que le pays tiers ou l'organisation internationale en question assure un niveau adéquat de protection ou, en l'absence de décision constatant le caractère adéquat de la protection conformément à l'article 34, des garanties appropriées ont été offertes ou existent conformément à l'article 35 ou, en l'absence à la fois de décision constatant le caractère adéquat de la protection conformément à l'article 34 et de garanties appropriées conformément à l'article 35, des dérogations pour des situations particulières s'appliquent conformément à l'article 36;

e *bis*) en cas de transfert ultérieur vers un autre pays tiers ou à une autre organisation internationale, l'autorité compétente qui a procédé au transfert initial ou une autre autorité compétente du même État membre autorise le transfert ultérieur, après avoir dûment pris en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction, la finalité pour laquelle les données ont été transférées initialement et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel/laquelle les données à caractère personnel sont transférées ultérieurement.

2. Les États membres font en sorte que les transferts effectués sans l'autorisation préalable d'un autre État membre prévue au paragraphe 1, point d), soient autorisés uniquement lorsque le transfert de données à caractère personnel est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre et si l'autorisation préalable ne peut pas être obtenue en temps utile. L'autorité à laquelle il revient d'accorder l'autorisation préalable est informée sans délai.

3 *bis*. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par la présente directive ne soit pas compromis.

Article 34

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

1. Les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, ou un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

2. Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte notamment des éléments suivants:

a) la primauté du droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, des règles en matière de protection des données, des règles professionnelles et des mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées;

b) l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, y compris par des pouvoirs de sanction appropriés, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres; et

c) les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants et de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

3. La Commission, après avoir évalué le caractère adéquat du niveau de protection, peut constater par voie de décision qu'un pays tiers, ou un territoire ou un ou plusieurs secteurs déterminés dans le pays tiers en question, ou une organisation internationale, assure un niveau de protection adéquat au sens du paragraphe 2. L'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale. L'acte d'exécution précise son champ d'application territorial et sectoriel et, le cas échéant, cite le nom de la ou des autorités de contrôle mentionnées au paragraphe 2, point b). L'acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 57, paragraphe 2.

4. (…)

4 *bis*. La Commission suit, de manière permanente, les évolutions dans les pays tiers et au sein des organisations internationales qui pourraient porter atteinte au fonctionnement des décisions adoptées en vertu du paragraphe 3.

5. La Commission constate par voie de décision, selon ce que révèlent les informations disponibles, en particulier à la suite de l'examen visé au paragraphe 3, qu'un pays tiers, ou un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat au sens du paragraphe 2 et, si nécessaire, abroge, modifie ou suspend la décision visée au paragraphe 3 sans effet rétroactif. L'acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 57, paragraphe 2, ou, en cas d'extrême urgence, en conformité avec la procédure visée à l'article 57, paragraphe 3.

5 *bis*. La Commission engage des consultations avec le pays tiers ou l'organisation internationale en vue de remédier à la situation donnant lieu à la décision adoptée en vertu du paragraphe 5.

6. Les États membres prévoient qu'une décision adoptée en vertu du paragraphe 5 est sans préjudice des transferts de données à caractère personnel vers le pays tiers, ou le territoire ou le secteur déterminé dans ce pays tiers, ou à l'organisation internationale en question, effectués au titre des articles 35 et 36.

7. La Commission publie au Journal officiel de l'Union européenne et sur son site web une liste des pays tiers, des territoires et des secteurs déterminés dans un pays tiers et des organisations internationales pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat est ou n'est plus assuré.

8. (…)

Article 35

Transferts moyennant des garanties appropriées

1. En l'absence de décision en vertu de l'article 34, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque:

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

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

1 *bis*. Le responsable du traitement informe l'autorité de contrôle des catégories de transferts relevant du paragraphe 1, point b).

2. Lorsqu'un transfert est effectué sur la base du paragraphe 1, point b), ce transfert doit être documenté et la documentation doit être mise à la disposition de l'autorité de contrôle, sur demande, et indiquer la date et l'heure du transfert, donner des informations sur l'autorité compétente destinataire, indiquer la justification du transfert et les données transférées.

Article 36

Dérogations pour des situations particulières

1. En l'absence de décision constatant le caractère adéquat de la protection en vertu de l'article 34 ou de garanties appropriées conformément à l'article 35, les États membres prévoient qu'un transfert ou une catégorie de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu que dans les conditions suivantes:

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

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

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

d) le transfert est nécessaire, dans des cas particuliers, aux fins énoncées à l'article 1er, paragraphe 1; ou

e) le transfert est nécessaire, dans un cas particulier, à la constatation, à l'exercice ou à la défense d'un droit en justice en rapport avec les fins énoncées à l'article 1er, paragraphe 1.

2. Les données à caractère personnel ne sont pas transférées si l'autorité compétente qui transfère les données estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert visé au paragraphe 1, points d) et e).

3. Lorsqu'un transfert est effectué sur la base du paragraphe 1, point b), ce transfert doit être documenté et la documentation doit être mise à la disposition de l'autorité de contrôle, sur demande, et indiquer la date et l'heure du transfert, donner des informations sur l'autorité compétente destinataire, indiquer la justification du transfert et les données transférées.

Article 36 bis bis

Transfert de données à caractère personnel à des destinataires établis dans des pays tiers

1. Par dérogation à l'article 33, paragraphe 1, point c), et sans préjudice de tout accord international visé au paragraphe 2 du présent article, le droit de l'Union ou la législation d'un État membre peut prévoir que les autorités compétentes au sens de l'article 3, point 14) a), peuvent, dans certains cas particuliers, transférer des données à caractère personnel directement aux destinataires établis dans des pays tiers, uniquement lorsque les autres dispositions de la présente directive sont respectées et que les conditions ci-après sont remplies:

a) le transfert est strictement nécessaire à l'exécution de la mission de l'autorité compétente qui transfère les données ainsi que le prévoit le droit de l'Union ou la législation d'un État membre aux fins énoncées à l'article 1er, paragraphe 1; et

b) l'autorité compétente qui transfère les données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui l'emportent sur l'intérêt public exigeant le transfert dans le cas en question; et

c) l'autorité compétente qui transfère les données estime que le transfert, aux fins visées à l'article 1er, paragraphe 1, à une autorité compétente dans le pays tiers est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun; et

d) l'autorité compétente dans le pays tiers est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié; et

e) l'autorité compétente qui transfère les données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel feront l'objet d'un traitement par ce dernier, lorsqu'un tel traitement est nécessaire.

2. Par accord international visé au paragraphe 1, on entend tout accord international bilatéral ou multilatéral en vigueur entre les États membres et des pays tiers dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière.

2 *bis*. L'autorité compétente qui transfère les données informe l'autorité de contrôle des transferts relevant du présent article.

2 *ter*. Lorsqu'un transfert est effectué sur la base du paragraphe 1, ce transfert doit être documenté.

Article 37

(...)

Article 38

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

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

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

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

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

   d) favoriser l'échange et la documentation de la législation et des pratiques en matière de protection des données à caractère personnel, y compris en ce qui concerne les conflits de compétence avec des pays tiers.

2. (…)

CHAPITRE VI
AUTORITÉS DE CONTRÔLE INDÉPENDANTES

SECTION 1
STATUT D'INDÉPENDANCE

Article 39

Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application de la présente directive, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement de leurs données à caractère personnel et de faciliter la libre circulation des données à caractère personnel au sein de l'Union.

1 *bis*. Chaque autorité de contrôle contribue à l'application cohérente de la présente directive dans l'ensemble de l'Union. À cette fin, les autorités de contrôle coopèrent entre elles et avec la Commission conformément au chapitre VII.

2. Les États membres peuvent prévoir qu'une autorité de contrôle instituée conformément au règlement (UE) …/XXX peut être l'autorité de contrôle visée dans la présente directive et prend en charge les missions de l'autorité de contrôle devant être instituée conformément au paragraphe 1 du présent article.

3. Lorsqu'un État membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité européen de la protection des données.

Article 40

Indépendance

1. Les États membres veillent à ce que chaque autorité de contrôle exerce en toute indépendance les missions et les pouvoirs qui lui sont confiés conformément à la présente directive.

2. Les États membres prévoient que, dans l'exercice de leurs missions et de leurs pouvoirs conformément à la présente directive, le membre ou les membres de chaque autorité de contrôle demeurent libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions de quiconque.

3. Les membres de l'autorité de contrôle s'abstiennent de tout acte incompatible avec leurs fonctions et, pendant la durée de leur mandat, n'exercent aucune activité professionnelle incompatible, rémunérée ou non.

4. (…)

5. Chaque État membre veille à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, notamment lorsqu'elle doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité européen de la protection des données.

6. Chaque État membre veille à ce que chaque autorité de contrôle choisisse et dispose de ses propres agents, qui sont placés sous les ordres exclusifs du membre ou des membres de l'autorité de contrôle.

7. Les États membres veillent à ce que chaque autorité de contrôle soit soumise à un contrôle financier qui ne menace pas son indépendance. Les États membres veillent à ce que chaque autorité de contrôle dispose d'un budget annuel public propre, qui peut faire partie du budget national ou du budget d'une entité fédérée.

Article 41

Conditions générales applicables aux membres de l'autorité de contrôle

1. Chaque État membre prévoit que chacun des membres d'une autorité de contrôle doit être nommé selon une procédure transparente soit par le parlement, soit par le gouvernement, soit par le chef d'État de l'État membre concerné, soit encore par un organisme indépendant chargé par la législation de l'État membre de procéder à la nomination.

2. Le membre ou les membres ont les qualifications, l'expérience et les compétences nécessaires, notamment dans le domaine de la protection des données à caractère personnel, pour l'exercice de leurs fonctions et de leurs pouvoirs.

3. Les fonctions d'un membre prennent fin à l'échéance de son mandat, en cas de démission ou de mise à la retraite d'office, conformément à la législation de l'État membre concerné.

4. Un membre ne peut être démis de ses fonctions que s'il a commis une faute grave ou s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions.

5. (…)

Article 42

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

1. Chaque État membre prévoit, par voie législative:

   a) la création de chaque autorité de contrôle;

   b) les qualifications et les conditions d'éligibilité requises pour être nommé membre de chaque autorité de contrôle;

   c) les règles et les procédures pour la nomination des membres de chaque autorité de contrôle;

d) la durée du mandat du membre ou des membres de chaque autorité de contrôle, qui n'est pas inférieure à quatre ans, sauf pour le premier mandat suivant l'entrée en vigueur de la présente directive, qui peut être d'une durée plus courte lorsque cela est nécessaire pour protéger l'indépendance de l'autorité de contrôle au moyen d'une procédure de nominations échelonnées;

e) le caractère renouvelable ou non renouvelable du mandat du membre ou des membres de chaque autorité de contrôle et, dans l'affirmative, pour combien de mandats;

f) les conditions régissant les obligations du membre ou des membres et des agents de chaque autorité de contrôle, les interdictions d'activités, d'emplois et d'avantages incompatibles avec celles-ci, y compris après la cessation de leurs activités, et les règles régissant la cessation de l'emploi.

g) (…)

1 *bis*. Le membre ou les membres et les agents de chaque autorité de contrôle sont soumis, conformément au droit de l'Union ou à la législation d'un État membre, au secret professionnel concernant toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs missions ou de leurs pouvoirs, y compris après la cessation de leurs activités. Pendant la durée de leur mandat, ce devoir de secret professionnel s'applique en particulier au signalement par des personnes physiques d'infractions à la présente directive.

Article 43

(...)

SECTION 2
COMPÉTENCE, MISSIONS ET POUVOIRS

Article 44

Compétence

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

2. Les États membres prévoient que l'autorité de contrôle n'est pas compétente pour contrôler les traitements effectués par les juridictions dans l'exercice de leur fonction juridictionnelle. Les États membres peuvent prévoir que l'autorité de contrôle n'est pas compétente pour contrôler les traitements effectués par d'autres autorités judiciaires indépendantes dans l'exercice de leur fonction juridictionnelle.

Article 45

Missions

1. Les États membres prévoient que, sur son territoire, chaque autorité de contrôle:

   a) contrôle l'application des dispositions adoptées en vertu de la présente directive et de ses mesures d'exécution et veille au respect de celles-ci;

   a *bis*) favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement des données à caractère personnel;

   a *ter*) conseille, conformément à la législation nationale, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel;

   a *quater*) encourage la sensibilisation des responsables du traitement et des sous-traitants en ce qui concerne les obligations qui leur incombent en vertu de la présente directive;

a *quinquies*) fournit, sur demande, à toute personne concernée, des informations sur l'exercice de ses droits découlant de la présente directive et, si nécessaire, coopère à cette fin avec les autorités de contrôle d'autres États membres;

b) traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association conformément à l'article 53, examine l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire;

c) vérifie la licéité du traitement de données en vertu de l'article 15 *bis* , et informe la personne concernée dans un délai raisonnable de l'issue de la vérification, conformément à l'article 15 *bis*, paragraphe 2, ou des motifs ayant empêché sa réalisation;

d) coopère avec d'autres autorités de contrôle, y compris en partageant des informations, et leur fournit une assistance mutuelle en vue d'assurer une application cohérente de la présente directive et des mesures prises pour en assurer le respect;

e) effectue des enquêtes sur l'application de la présente directive, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique;

f) suit les évolutions présentant un intérêt, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et de la communication;

g) (…)

h) fournit des conseils sur les opérations de traitement visées à l'article 26;

i) contribue aux activités du comité européen de la protection des données.

2. (…)

3. (…)

4. Chaque autorité de contrôle facilite l'introduction des réclamations visées au paragraphe 1, point b), par des mesures telles que la fourniture d'un formulaire de réclamation qui peut être rempli également par voie électronique, sans que d'autres moyens de communication soient exclus.

5. L'accomplissement des missions de chaque autorité de contrôle est gratuit pour la personne concernée et pour le délégué à la protection des données.

6. Lorsque les demandes sont manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif, l'autorité de contrôle peut exiger le paiement de frais raisonnables basés sur les coûts administratifs ou refuser de donner suite à la demande. Il incombe à l'autorité de contrôle de démontrer le caractère manifestement infondé ou excessif de la demande.

Article 46

Pouvoirs

1. Chaque État membre prévoit, par voie législative, que son autorité de contrôle dispose de pouvoirs d'enquête effectifs, au moins du pouvoir d'obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel qui sont traitées et à toutes les informations nécessaires à l'exercice de ses missions.

   a) (…)

   b) (…)

   c) (…)

1 *bis*. Chaque État membre prévoit, par voie législative, que son autorité de contrôle dispose de pouvoirs effectifs en matière d'adoption de mesures correctrices, tels que, par exemple:

   a) avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions adoptées en vertu de la présente directive;

b) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions adoptées en vertu de la présente directive, le cas échéant, de manière spécifique et dans un délai déterminé; en particulier en ordonnant la rectification ou l'effacement de données ou la limitation de leur traitement en application de l'article 15;

c) limiter temporairement ou définitivement, y compris interdire, un traitement.

1 *ter*. Chaque État membre prévoit, par voie législative, que son autorité de contrôle dispose des pouvoirs consultatifs effectifs de conseiller le responsable du traitement conformément à la procédure de consultation préalable visée à l'article 26 et d'émettre, de sa propre initiative ou sur demande, des avis à l'attention du parlement national, du gouvernement de l'État membre ou, conformément à la législation nationale, d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel.

2. L'exercice des pouvoirs conférés à l'autorité de contrôle en application du présent article est subordonné à des garanties appropriées, y compris le droit à un recours effectif et à une procédure régulière, prévues par le droit de l'Union et la législation d'un État membre conformément à la charte des droits fondamentaux de l'Union européenne.

3. Chaque État membre prévoit, par voie législative, que son autorité de contrôle a le pouvoir de porter les violations des dispositions adoptées en vertu de la présente directive à la connaissance de l'autorité judiciaire et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire respecter les dispositions adoptées en vertu de la présente directive.

Article 46 bis

Signalement des infractions

Les États membres prévoient que les autorités compétentes mettent en place des mécanismes efficaces pour encourager le signalement confidentiel des infractions à la présente directive.

Article 47

Rapport d'activité

Chaque autorité de contrôle établit un rapport annuel sur ses activités, qui peut comprendre une liste des types d'infractions notifiées et des types de sanctions imposées. Le rapport est transmis au parlement national, au gouvernement et à d'autres autorités désignées par la législation nationale. Il est mis à la disposition du public, de la Commission et du comité européen de la protection des données.

CHAPITRE VII
COOPÉRATION

Article 48

Assistance mutuelle

1. Les États membres prévoient que les autorités de contrôle se communiquent les informations utiles et se prêtent une assistance mutuelle en vue de mettre en œuvre et d'appliquer la présente directive de façon cohérente, et mettent en place des mesures pour coopérer efficacement. L'assistance mutuelle commune notamment les demandes d'information et les mesures de contrôle, telles que les demandes de consultation, les inspections et les enquêtes.

2. Les États membres prévoient que chaque autorité de contrôle prend toutes les mesures appropriées requises pour répondre à la demande d'une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande. Il peut s'agir notamment de la transmission d'informations utiles sur la conduite d'une enquête.

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

2 *ter*. Une autorité de contrôle saisie d'une demande d'assistance ne peut refuser d'y donner suite, sauf si:

a) elle n'est pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter; ou

b) y donner suite serait incompatible avec les dispositions de la présente directive ou avec le droit de l'Union ou la législation de l'État membre à laquelle l'autorité de contrôle qui a reçu la demande est soumise.

3. L'autorité de contrôle requise informe l'autorité de contrôle requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour donner suite à la demande. Lorsqu'elle refuse de donner suite à une demande en application du paragraphe 2 *ter*, elle explique les raisons de son refus.

3 *bis*. En règle générale, les autorités de contrôle communiquent par voie électronique et au moyen d'un formulaire type, les informations demandées par d'autres autorités de contrôle.

3 *ter*. Une mesure prise à la suite d'une demande d'assistance mutuelle ne donne pas lieu à la perception de frais. Les autorités de contrôle peuvent convenir, avec d'autres autorités de contrôle, de règles relatives à l'octroi, par d'autres autorités de contrôle, de dédommagements concernant des dépenses spécifiques résultant de la fourniture d'une assistance mutuelle dans des circonstances exceptionnelles.

3 *quater*. La Commission peut préciser la forme et les procédures de l'assistance mutuelle visée au présent article, ainsi que les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle et entre les autorités de contrôle et le comité européen de la protection des données. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 57, paragraphe 2.

Article 49

Missions du comité européen de la protection des données

1. Le comité européen de la protection des données institué par le règlement (UE) ..../ XXX accomplit les missions ci-après en ce qui concerne les activités de traitement relevant du champ d'application de la présente directive:

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

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

b *bis*) élaborer, à l'intention des autorités de contrôle, des lignes directrices concernant l'application des mesures visées à l'article 46, paragraphes 1 et 1 *ter*;

b *ter*) publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point b) du présent paragraphe, en vue d'établir les violations de données à caractère personnel et de déterminer les meilleurs délais visés à l'article 28, paragraphes 1 et 2, et de préciser les circonstances particulières dans lesquelles un responsable du traitement ou un sous-traitant est tenu de notifier la violation des données à caractère personnel;

b *quater*) publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point b) du présent paragraphe concernant les circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique, comme le prévoit l'article 29, paragraphe 1;

c) faire le bilan de l'application pratique des lignes directrices, des recommandations et des bonnes pratiques visées aux points b) et b *bis*);

d) rendre à la Commission un avis en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers ou une organisation internationale, y compris concernant l'évaluation visant à déterminer si un pays tiers, le territoire, l'organisation internationale ou un secteur déterminé n'assure plus un niveau adéquat de protection. À cette fin, la Commission fournit au comité européen de la protection des données tous les documents nécessaires, y compris la correspondance avec le gouvernement du pays tiers, le territoire ou le secteur du traitement dans ce pays tiers, ou avec l'organisation internationale;

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

f) promouvoir l'élaboration de programmes de formation conjoints et faciliter les échanges de personnel entre autorités de contrôle, ainsi que, le cas échéant, avec les autorités de contrôle de pays tiers ou d'organisations internationales;

g) promouvoir l'échange, avec des autorités de contrôle de la protection des données de tous pays, de connaissances et de documentation sur la législation et les pratiques en matière de protection des données.

2. Lorsque la Commission demande conseil au comité européen de la protection des données, elle peut mentionner un délai, selon l'urgence de la question.

3. Le comité européen de la protection des données transmet ses avis, lignes directrices, recommandations et bonnes pratiques à la Commission et au comité visé à l'article 57, paragraphe 1, et les publie.

4. La Commission informe le comité européen de la protection des données des suites qu'elle a réservées aux avis, lignes directrices, recommandations et bonnes pratiques publiés par ledit comité.

CHAPITRE VIII
VOIES DE RECOURS, RESPONSABILITÉ ET SANCTIONS

Article 50

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

1. Sans préjudice de tout autre recours administratif ou juridictionnel, les États membres prévoient que toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle unique, si elle considère que le traitement de données à caractère personnel la concernant n'est pas conforme aux dispositions adoptées en vertu de la présente directive.

1 *bis*. Les États membres prévoient que, si la réclamation n'est pas introduite auprès de l'autorité de contrôle compétente au titre de l'article 44, paragraphe 1, l'autorité de contrôle auprès de laquelle la réclamation a été introduite la transmet sans tarder à l'autorité de contrôle compétente. La personne concernée est informée de cette transmission.

1 *ter*. Les États membres prévoient que l'autorité de contrôle auprès de laquelle la réclamation a été introduite fournit une assistance supplémentaire à la demande de la personne concernée.

2. (…)

2 *bis*. La personne concernée est informée par l'autorité de contrôle compétente de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article 51.

3. (…)

Article 51

Droit à un recours juridictionnel effectif contre une autorité de contrôle

1. Sans préjudice de tout autre recours administratif ou extrajudiciaire, les États membres prévoient qu'une personne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne.

2. Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit de former un recours juridictionnel effectif lorsque l'autorité de contrôle compétente au titre de l'article 44, paragraphe 1, ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite conformément à l'article 50.

3. Les États membres prévoient que les actions contre une autorité de contrôle sont intentées devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie.

Article 52

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

Les États membres prévoient que, sans préjudice de tout recours administratif ou extrajudiciaire qui leur est ouvert, notamment le droit d'introduire une réclamation auprès d'une autorité de contrôle conformément à l'article 50, les personnes concernées ont droit à un recours juridictionnel effectif si elles considèrent qu'il a été porté atteinte aux droits que leur confèrent les dispositions adoptées en vertu de la présente directive du fait que le traitement de données à caractère personnel les concernant a été effectué en violation desdites dispositions.

Article 53

Représentation des personnes concernées

1. Les États membres prévoient, conformément au droit procédural national, que la personne concernée a le droit de mandater un organisme, une organisation ou une association, qui a été valablement constitué conformément à la législation d'un État membre, qui est à but non lucratif, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel la concernant, pour qu'il introduise une réclamation en son nom et exerce en son nom les droits visés aux articles 50, 51 et 52.

2. (…)

3. (…)

Article 54

Droit à réparation

1. Les États membres prévoient que toute personne ayant subi un dommage matériel ou immatériel du fait d'une opération de traitement illicite ou de toute action incompatible avec les dispositions nationales adoptées en vertu de la présente directive a le droit d'obtenir du responsable du traitement, ou de toute autre autorité compétente en vertu de la législation nationale, réparation du préjudice subi.

2. (…)

3. (…)

Article 55

Sanctions

Les États membres déterminent le régime des sanctions applicables en cas d'infractions aux dispositions adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Les sanctions ainsi prévues doivent être effectives, proportionnées et dissuasives.

CHAPITRE IX
ACTES D'EXÉCUTION

Article 56

(...)

Article 57

Comité

1. La Commission est assistée par le comité institué par l'article 87 du règlement (UE) ..../XXX. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 8 du règlement (UE) n° 182/2011 s'applique, en liaison avec son article 5.

CHAPITRE X
DISPOSITIONS FINALES

Article 58

Abrogation

1. La décision-cadre 2008/977/JAI du Conseil est abrogée à compter de la date visée à l'article 62, paragraphe 1.

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

Article 59

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

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

Article 60

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

Les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales qui ont été conclus par les États membres avant l'entrée en vigueur de la présente directive et qui sont conformes au droit de l'Union applicable avant l'entrée en vigueur de la présente directive restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation.

Article 61

Évaluation

1. La Commission présente périodiquement au Parlement européen et au Conseil des rapports sur l'évaluation et le réexamen de la présente directive.

1 *bis*. Dans le cadre de ces évaluations et réexamens, la Commission examine, en particulier, l'application et le fonctionnement des dispositions du chapitre V sur le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, en accordant une attention particulière aux décisions adoptées en vertu de l'article 34, paragraphe 3, et de l'article 36 *bis bis*.

1 *ter*. Aux fins visées aux paragraphes 1 et 1 *bis*, la Commission peut demander des informations aux États membres et aux autorités de contrôle.

1 *quater*. Lorsqu'elle procède aux évaluations et réexamens visés aux paragraphes 1 et 1 *bis*, la Commission tient compte des positions et des conclusions du Parlement européen, du Conseil ainsi que d'autres organismes ou sources pertinents.

1 *quinquies*. Le premier rapport est présenté au plus tard quatre ans après l'entrée en vigueur de la présente directive. Les rapports suivants sont ensuite présentés tous les quatre ans. Les rapports sont publiés.

1 *sexies*. La Commission soumet, si nécessaire, les propositions appropriées pour modifier la présente directive et adapter d'autres instruments juridiques, notamment en tenant compte de l'évolution des technologies de l'information et des progrès de la société de l'information.

2. Dans un délai de trois ans à compter de l'entrée en vigueur de la présente directive, la Commission réexamine d'autres actes adoptés par l'Union européenne qui régissent le traitement des données à caractère personnel par les autorités compétentes aux fins énoncées à l'article 1er, paragraphe 1, y compris les actes adoptés par l'Union qui sont visés à l'article 59, afin d'apprécier la nécessité de les mettre en conformité avec la présente directive et de formuler, le cas échéant, les propositions nécessaires en vue de modifier ces actes pour assurer une approche cohérente de la protection des données à caractère personnel dans le cadre de la présente directive.

3. (…)

Article 62

Transposition

1. Les États membres adoptent et publient, au plus tard le [date/deux ans après l'entrée en vigueur], les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils communiquent immédiatement à la Commission le texte de ces dispositions. Ils appliquent ces dispositions à partir du xx.xx.201x [date/deux ans après l'entrée en vigueur].

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

1 *bis*. Par dérogation au paragraphe 1, les États membres peuvent prévoir que, à titre exceptionnel, lorsque cela exige des efforts disproportionnés, les systèmes de traitement automatisé installés avant la date d'entrée en vigueur de la présente directive sont mis en conformité avec l'article 24, paragraphe 1, dans un délai de sept ans à compter de la date d'entrée en vigueur de la présente directive.

1 *ter*. Dans des circonstances exceptionnelles, un État membre peut mettre un système donné de traitement automatisé, installé avant la date d'entrée en vigueur de la présente directive, en conformité avec l'article 24, paragraphe 1, dans un délai déterminé après le délai visé au paragraphe 1 *bis*, lorsque, à défaut de cela, de graves difficultés se poseraient pour le fonctionnement du système de traitement automatisé en question. Il notifie à la Commission les raisons de ces graves difficultés et les motifs justifiant le délai déterminé de mise en conformité du système donné de traitement automatisé avec l'article 24, paragraphe 1. Le délai déterminé n'est en aucun cas supérieur à trois ans après le délai visé au paragraphe 1 *bis*.

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

Article 63

Entrée en vigueur

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

Article 64

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à …, le …

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