

Bruxelles, le 2 octobre 2015  
(OR. en)

12555/15

---

---

**Dossier interinstitutionnel:  
2012/0010 (COD)**

---

---

**DATAPROTECT 154  
JAI 707  
DAPIX 163  
FREMP 202  
COMIX 456  
CODEC 1279**

## NOTE

---

Origine:	la présidence
Destinataire:	Conseil
N° doc. préc.:	12266/15
N° doc. Cion:	5833/12
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 - Orientation générale

---

## I. INTRODUCTION

1. Le 27 janvier 2012, la Commission a présenté 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 (ci-après dénommée le projet de directive).<sup>1</sup> Cette proposition vise à remplacer la décision-cadre 2008/977/JAI.<sup>2</sup>

---

<sup>1</sup> Doc. 5833/12.

<sup>2</sup> JO L 350 du 30.12.2008, p. 60.

2. Parallèlement à cette proposition de directive, la Commission a présenté une proposition de règlement général sur la protection des données (ci-après dénommé le projet de règlement)<sup>3</sup> destiné à remplacer la directive 95/46/CE.<sup>4</sup> Ces projets de directive et de règlement constituent le train de mesures visant à réformer le cadre juridique de la protection des données.
3. Le Parlement européen a adopté sa position en première lecture concernant le projet de directive le 12 mars 2014 dans le cadre de la procédure législative ordinaire.<sup>5</sup>
4. Le contrôleur européen de la protection des données a rendu son avis sur la proposition de la Commission le 8 mars 2012.<sup>6</sup>
5. Le groupe "Échange d'informations et protection des données" (DAPIX) a commencé à examiner le texte lors de sa réunion du 16 avril 2012, sous présidence danoise. Le projet de directive a depuis lors été discuté au sein du DAPIX pendant chaque présidence.
6. Pendant la présidence luxembourgeoise, depuis juillet 2015, le projet de directive a été discuté aux réunions du DAPIX ainsi qu'à l'occasion des réunions des Amis de la présidence des 2-3 juillet, 15-16 juillet, 22 juillet, 3-4 septembre, 9 septembre, 16 septembre, et 21-22 septembre, à celle des conseillers JAI du 28 septembre et au Coreper les 24 septembre et 1<sup>er</sup> octobre 2015.
7. Le Conseil européen a demandé dans ses conclusions des 25-26 juin 2015 que le paquet relatif à la protection des données soit adopté d'ici la fin de l'année 2015.<sup>7</sup>
8. Lors de sa session du 15 juin 2015, le Conseil a adopté son orientation générale sur le projet de règlement. Les négociations avec le Parlement européen sur le règlement vont bon train et sont menées dans un esprit de compromis.

---

<sup>3</sup> Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (doc. 5853/12).

<sup>4</sup> Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. JO L 281 du 23.11.1995, p. 31.

<sup>5</sup> Doc. 7428/14.

<sup>6</sup> Doc. 7375/12.

<sup>7</sup> Voir doc. EUCO 22/15, point 12, a).

9. Compte tenu de ce qui précède, la présidence s'est engagée à faire aboutir en 2015 les négociations sur les deux propositions de ce paquet.
10. On a beaucoup progressé sur le texte du projet de directive depuis le 1<sup>er</sup> juillet 2015. La présidence estime que le texte est prêt à être soumis aux ministres, qui pourront confirmer l'orientation générale afin que les négociations avec le Parlement européen puissent commencer sur cette base.

## II. TEXTE DE COMPROMIS

11. Le texte du projet de directive que la présidence présente en vue d'une orientation générale figure en annexe. Toutes les modifications apportées à la proposition initiale de la Commission apparaissent en caractères soulignés; les passages supprimés sont remplacés par des parenthèses (...). Le texte existant qui a été déplacé est en *italique*. Les commentaires des délégations sur le texte du projet de directive - qui ne contenait pas encore les modifications des considérants 18, 27, 36, 57 et 71 et des articles 61 et 62 - sont reflétés dans les résultats des travaux menés par le Comité des représentants permanents lors de sa réunion du 1<sup>er</sup> octobre 2015 (doc. 12643/15).
12. Tenant compte de ce qui a été dit lors de la réunion du Comité des représentants permanents du 1<sup>er</sup> octobre 2015 et soucieuse de répondre aux dernières préoccupations des délégations, la présidence a apporté les changements ci-après au texte du projet de directive:
  - i. Au considérant 18, les termes "pour les besoins de la présente directive" ont été supprimés.
  - ii. Au considérant 27, le terme "et" est remplacé par "ou".
  - iii. Au considérant 36, le terme "temporairement" a été supprimé et les termes "en pareil cas" ont été ajoutés.
  - iv. Au considérant 57, une phrase a été ajoutée pour indiquer que les pouvoirs des autorités de contrôle ne devraient pas interférer avec des règles spécifiques de procédure pénale ni avec l'indépendance du pouvoir judiciaire.

- v. L'article 61 a été modifié pour indiquer que, lorsque la Commission évalue l'application de la directive, elle devrait aussi évaluer, en particulier, le fonctionnement de l'article 36 *bis bis*.
- vi. Le délai fixé à l'article 62 (et au considérant 71) pour la mise en œuvre a été porté à trois ans.

### III. CONCLUSION

- 13. Compte tenu de ce qui précède et dans un esprit de compromis en vue de donner à la présidence un mandat pour engager des négociations avec les représentants du Parlement européen, le Conseil est invité à confirmer l'orientation générale sur le texte du projet de directive tel qu'il figure dans l'annexe de la présente note.
-

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, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de prévention de telles menaces, et à la libre circulation de ces données**

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

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

vu la proposition de la Commission européenne,

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

après consultation du contrôleur européen de la protection des données<sup>8</sup>,

---

<sup>8</sup> JO C [...] du [...], p. [...].

statuant conformément à la procédure législative ordinaire,  
considérant ce qui suit:

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

(2) 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 leurs droits fondamentaux, notamment le droit à la protection des données à caractère personnel. Le traitement des données devrait contribuer à la réalisation d'un espace de liberté, de sécurité et de justice.

(3) La rapide évolution des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. La collecte et le partage de données ont connu une augmentation spectaculaire. Les nouvelles technologies permettent (...) 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, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de 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<sup>9</sup> 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.

---

<sup>9</sup> 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<sup>10</sup> 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, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de prévention de telles menaces devrait être équivalent dans tous les États membres. Une protection effective des données à caractère personnel dans toute l'Union exige non seulement de renforcer les droits des personnes concernées et les obligations de ceux qui traitent ces données, mais aussi de conférer, dans les États membres, des pouvoirs équivalents de surveillance et de contrôle de l'application des règles relatives à la protection des données à caractère personnel.

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

(9) Sur cette base, le règlement (UE) .../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.

---

<sup>10</sup> 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*. 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 organisme/entité à qui la législation nationale confie l'exercice de fonctions publiques ou de prérogatives publiques 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. Toutefois, lorsqu'un tel organisme ou une telle entité traite des données à caractère personnel à des fins autres que l'exercice de fonctions publiques ou de prérogatives publiques en matière de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière *ou d'exécution de sanctions pénales*, 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 le droit national. 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 effectuées 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 effectuées 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 de prévention de telles menaces, en vue d'empêcher les comportements de nature à nuire aux intérêts fondamentaux de la société protégés par la loi et 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 et de poursuites en la matière ou de protection contre les menaces pour la sécurité publique et de 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 n'entrant pas dans le 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 toute l'Union et d'éviter que des différences n'entravent les échanges de données à caractère personnel entre les autorités (...) compétentes, la directive devrait prévoir des règles harmonisées pour la protection et la libre circulation des données à caractère personnel (...) traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de 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 tâche réalisée dans l'intérêt public peuvent être communiquées par cette autorité ou cet organisme conformément au droit de l'Union ou 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) n° 45/2001<sup>11</sup> s'applique au traitement des données à caractère personnel par les institutions, organes, organismes et agences de l'Union. Le règlement (CE) n° 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.

---

<sup>11</sup> JO L 8 du 12.1.2001, p. 1.

(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 tribunaux 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 susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier directement ou indirectement ladite 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.

(16 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. (...)

(17) Les données à caractère personnel concernant la santé devraient comprendre (...) les données se rapportant à l'état de santé d'une personne concernée qui comportent des informations sur la santé physique ou mentale passée, présente ou future de la personne concernée, (...) y compris des informations (...) relatives à l'enregistrement du patient pour la prestation de services de santé, un numéro ou un symbole attribué à un patient, destinés à 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'une épreuve diagnostique in vitro.

(18) Tout traitement de données à caractère personnel devrait être (...) licite et loyal à l'égard des personnes concernées et n'être effectué qu'aux fins spécifiques fixées par la loi. Le principe de traitement loyal 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 ou de protection contre les menaces pour la sécurité publique et de 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. Les personnes devraient être informées des risques, règles, garanties et droits relatifs au traitement des données à caractère personnel 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'une révision 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 ou 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 phénomènes criminels et des tendances qui les caractérisent, recueillir des renseignements sur les réseaux criminels organisés et établir des liens entre les différentes infractions mises au jour.

(19 bis) Afin de garantir la sécurité du traitement et d'empêcher 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 actuel des connaissances et de la technique 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, d'enquêtes et de poursuites en la matière, de l'exécution de sanctions pénales ou de la protection contre les menaces pour la sécurité publique et de 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 conviendrait d'appliquer le principe d'exactitude des données en tenant compte de la nature et de l'objet du traitement concerné. Étant donné que les données à caractère personnel traitées peuvent se rapporter à différentes catégories de personnes concernées, il convient que les autorités (...) compétentes établissent, dans la mesure du possible, une distinction entre les données à caractère personnel concernant différentes catégories de personnes, telles que les suspects, les personnes reconnues coupables d'une infraction pénale, les victimes et les tiers. Dans le cadre des procédures judiciaires, notamment, les déclarations contenant des données à caractère personnel sont, en effet, fondées sur des perceptions personnelles subjectives et ne sont pas toujours vérifiables. Ce principe ne devrait donc pas s'appliquer à l'exactitude de la déclaration elle-même mais simplement au fait qu'une certaine déclaration a été faite.

(22) Dans l'interprétation et l'application des dispositions de la présente directive (...) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de prévention de telles menaces, il convient de tenir compte des particularités du domaine, y compris des objectifs spécifiques poursuivis.

(23) (...)

(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 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, 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.

(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, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de 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, telles 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) .../XXXX devrait s'appliquer au traitement de ces données pour 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 nationale (...). 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 à qui 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 d'un État membre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de prévention de telles menaces, y compris le traitement nécessaire (...) à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne (...). Dans le cadre de l'exécution de 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 concernées 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 pénales 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 le droit national 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 (...) 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 à des destinataires dans des pays tiers ou des organisations internationales. Les États membres devraient prévoir 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 différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État membre dans lequel ladite autorité est établie.

(26) Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux (...) méritent une protection spécifique, car le contexte dans lequel elles sont traitées peut entraîner des risques importants pour les libertés et les droits fondamentaux. 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.

(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.

(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 aux données, leur rectification, leur effacement et la limitation de leur traitement. Le responsable du traitement devrait être tenu de répondre à la personne concernée sans tarder. Toutefois, 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 pourrait refuser de donner suite à la demande. (...)

(30) (...) Les informations suivantes, au moins, devraient être communiquées à la personne concernée: (...) l'identité du responsable du traitement, l'existence du traitement, (...) les finalités du traitement, (...) ainsi que (...) le droit d'introduire une réclamation. (...) Ces informations pourraient figurer sur le site web de l'autorité compétente.

(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 elle fait 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. (...) Pour que ce droit soit respecté, il suffit que la personne introduisant la demande 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.

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

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

(35) (...)

(36) Une personne physique devrait avoir le droit de faire rectifier des données à caractère personnel inexacts 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 (...) peut aussi avoir le droit de faire limiter le traitement (...) d'une donnée à caractère personnel la concernant lorsque son exactitude est contestée. 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 systèmes de 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 système.

(36 bis) Lorsque le responsable du traitement refuse à une personne concernée le droit d'accès, de rectification, d'effacement ou 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 intervient 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. (...)

(36 bis bis) Lorsque les données à caractère personnel sont traitées dans le cadre d'une enquête judiciaire ou d'une procédure judiciaire 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 les mesures appropriées et soit à même de démontrer (...) la conformité des activités de traitement avec les (...) dispositions adoptées en vertu de 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 concernées. Lorsqu'elles sont proportionnées aux activités de traitement de données, les mesures devraient comprendre la mise en œuvre de politiques appropriées en matière de protection des données. Ces politiques devraient préciser les modalités d'application des dispositions en matière de protection des données adoptées en vertu de la présente directive.

(37 bis) (...) Des risques pour les droits et libertés des personnes concernées, aux degrés de probabilité et de gravité variables, 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 ou concernant la santé ou la vie sexuelle, 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 personnelles ou les intérêts, 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 concernées à l'égard du traitement des données à caractère personnel les concernant exige l'adoption de mesures techniques et organisationnelles appropriées, pour satisfaire aux exigences prévues par la présente directive. Afin d'être en mesure de démontrer la conformité avec les dispositions adoptées en vertu de la présente directive, le responsable du traitement devrait adopter des règles internes et appliquer des mesures appropriées, qui répondent en particulier aux principes de la protection des données dès la conception et de la protection des données par défaut. Ces 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 utiles 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 de leurs sous-traitants, y compris dans le cadre de la surveillance exercée par les autorités de contrôle et des mesures prises par elles, exige une répartition claire des responsabilités au titre 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.

(40) Les catégories d'activités de traitement de données à caractère personnel prévoyant des transferts moyennant des garanties appropriées et effectuées dans des situations particulières devraient être inscrites dans un registre par le responsable du traitement (...) et le sous-traitant, afin de permettre un contrôle de la conformité du traitement avec la présente directive. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ce registre à sa disposition sur demande pour qu'ils servent au contrôle des traitements.

(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, l'interconnexion ou l'effacement. Les journaux devraient être utilisés à des fins de vérification de la licéité du traitement des données, d'autocontrôle et de garantie de l'intégrité et de la sécurité des données. (...) Cela n'empêche pas l'utilisation de journaux (...) conformément à la législation nationale pour des questions opérationnelles dans le cadre d'enquêtes et de procédures pénales.

(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 envisagé.

(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, une atteinte à la réputation, un renversement non autorisé de la procédure de pseudonymisation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social important. En conséquence, dès que le responsable du traitement apprend qu'une (...) violation de données à caractère personnel susceptible (...) de causer un dommage physique, matériel ou moral s'est produite, il convient qu'il en informe l'autorité de contrôle sans tarder. Les personnes physiques dont (...) les droits et libertés (...) pourraient être gravement affectés par la violation devraient en être informées dans les meilleurs délais afin de pouvoir prendre les précautions qui s'imposent (...).

(43) La communication à la personne concernée d'une violation de ses données à caractère personnel ne devrait pas être requise si le responsable du traitement a mis en œuvre les mesures de protection technologiques appropriées et si ces dernières ont été appliquées aux données concernées par ladite violation. Ces mesures de protection technologiques devraient inclure celles qui rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès, notamment par le cryptage des données à caractère personnel. De même, la communication à la personne concernée n'est pas requise si le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé au regard des droits et des libertés des personnes concernées n'est plus susceptible de (...) se matérialiser.

(44) (...) Une personne possédant des connaissances spécialisées de la législation et des pratiques en matière de protection des données peut aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, des dispositions adoptées en vertu de la présente directive. Cette personne peut informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les salariés traitant des données à caractère personnel sur les obligations qui leur incombent en matière de protection des données. Un délégué à la protection des données peut être désigné conjointement par plusieurs autorités ou organismes (...) compétents, compte tenu de leur structure organisationnelle et de leur taille (...). Ces délégués à la protection des données doivent être en mesure d'accomplir leurs missions et obligations (...) en toute indépendance.

(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*, ou (...) de protection contre les menaces pour la sécurité publique et de 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 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.

*(45 bis) Lorsque des données à caractère personnel sont transférées d'un État membre vers des États 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 État 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 l'État 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.*

(46) Lorsqu'elle n'a pas adopté de décision en application de l'article 41 du règlement (UE) .../XXX, la Commission peut décider, avec effet dans l'ensemble de l'Union, que certains pays tiers, 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 toute 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.

(47) Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait prendre en considération la manière dont un pays tiers déterminé 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 dans le cadre de 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.

(48) La Commission devrait également pouvoir constater qu'un pays tiers, 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 aux articles 35 et 36 soient respectées. Il y aurait lieu de prévoir des procédures de consultation entre la Commission et le pays tiers ou l'organisation internationale. 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) (...)

(49 bis bis) En l'absence de garanties appropriées ou de décision constatant le caractère adéquat de la protection, 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 préservation des intérêts légitimes de la personne concernée, si le droit de l'État membre qui transfère les données à caractère personnel le prévoit, ou à la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers, ou, dans certains cas, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution des sanctions pénales (...) ou à 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.

(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 de remplir les missions que leur confie la loi. En principe, ce processus se déroule en coopération avec les autorités compétentes des pays tiers concernés ou, à tout le moins, avec leur coopération. Cependant, dans certains cas particuliers, il se peut que les procédures prévues par les accords internationaux applicables ne permettent pas d'échanger en temps utile les informations nécessaires et que les autorités compétentes des États membres doivent donc transférer les données à caractère personnel directement à des destinataires situés dans des pays tiers. C'est notamment le cas (...) lorsque des infractions pénales ont été commises au moyen d'une technologie de communication électronique comme les réseaux sociaux ou lorsque des données générées par une technologie de communication peuvent servir d'éléments prouvant qu'une infraction pénale a été commise ou 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. Même si ces échanges (...) entre autorités compétentes et destinataires situés dans des pays tiers (...) ne devraient 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) (...)

(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 uniforme dans l'ensemble de l'Union, pour protéger les personnes physiques à l'égard du traitement de leurs données à caractère personnel. À cet effet, il conviendrait que les autorités de contrôle coopèrent entre elles et avec la Commission.

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

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

(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 chef d'État de l'État membre concerné, ou par un organisme indépendant chargé par la législation de l'État membre de procéder à la nomination selon une procédure transparente (...).

(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 aux traitements de données à caractère personnel effectués par les juridictions dans le cadre de leur fonction juridictionnelle, afin de préserver l'indépendance des juges dans l'exercice de leurs fonctions judiciaires. Il 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 du droit national. (...) 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 leurs fonctions juridictionnelles, 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'UE.

(56) *Chaque autorité devrait traiter les réclamations des personnes concernées et examiner les affaires en question. L'enquête faisant suite à une réclamation devrait être menée, sous contrôle juridictionnel, dans la mesure appropriée requise par l'affaire. L'autorité de contrôle devrait informer la personne concernée de l'état d'avancement et 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 la cohérence du contrôle et de l'application de la présente directive dans l'ensemble de l'Union, les autorités de contrôle devraient avoir, *dans chaque État membre*, les mêmes missions et les mêmes pouvoirs effectifs, dont celui d'enquêter, (...) d'adopter des mesures correctrices (...) et de délibérer. 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 droit national, 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 du droit national, 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'exercice 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 toute l'Union, notamment en conseillant la Commission et en favorisant la coopération des autorités de contrôle dans l'ensemble de l'Union.

(60) Toute personne concernée (...) devrait avoir le droit d'introduire une réclamation auprès d'une autorité de contrôle 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 une réclamation, si elle 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, de pouvoirs correctifs et de pouvoirs d'autorisation ou la révocation 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 au droit (...) national 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, une organisation ou une association qui œuvrent à la protection des droits et intérêts des personnes concernées dans le domaine de la protection des données et qui sont constitués conformément au droit national, (...) pour qu'ils introduisent une réclamation en son nom (...) (...) auprès d'une autorité de contrôle ou pour qu'ils exercent 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 conformément à la présente directive devrait être réparé par le responsable du traitement ou toute autre autorité compétente en vertu du droit national (...). 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 d'un État membre.

Lorsqu'il est fait référence à un traitement illicite ou non conforme aux dispositions adoptées conformément à 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 les dispositions adoptées conformément à 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 mesures nécessaires à leur application.

(66) (...)

(67) Afin de garantir des conditions uniformes pour la mise en œuvre de la présente directive, il convient de conférer des compétences d'exécution à la Commission en ce qui concerne: (...) le niveau adéquat de protection atteint par un pays tiers, un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale; 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 conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission<sup>12</sup>.

(68) (...) La procédure d'examen devrait être appliquée pour l'adoption d'actes d'exécution concernant (...) le niveau adéquat de protection atteint par un pays tiers, un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale; 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, (...) puisque ces actes sont de portée générale.

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

(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 réalisés de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

---

<sup>12</sup> JO L 55 du 28.2.2011, p. 13

(71) La décision-cadre 2008/977/JAI devrait être abrogée par 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 trois ans après son entrée en vigueur. Toutefois, lorsque ces traitements ont lieu en conformité avec la législation 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.

(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 demeurer 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<sup>13</sup> 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)<sup>14</sup>. La Commission devrait évaluer la situation en ce qui concerne la relation entre la présente directive et les actes adoptés avant la date de son adoption qui régissent le traitement des données à caractère personnel entre États membres ou l'accès d'autorités désignées des États membres aux systèmes d'information créés en vertu des traités, afin d'apprécier la nécessité de mettre ces dispositions spécifiques en conformité avec la présente directive.

(73) Afin d'assurer une protection exhaustive et cohérente des données à caractère personnel dans l'Union, il convient que les conventions et 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 abrogés. (...).

(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.<sup>15</sup>

---

<sup>13</sup> 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.

<sup>14</sup> 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).

<sup>15</sup> 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<sup>16</sup>.

(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<sup>17</sup>.

---

<sup>16</sup> JO L 176 du 10.7.1999, p. 36.

<sup>17</sup> JO L 53 du 27.2.2008, p. 52.

(79) En ce qui concerne le Liechtenstein, la présente directive constitue un développement des dispositions de l'acquis de Schengen au sens du protocole signé entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen<sup>18</sup>.

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

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

(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.

---

<sup>18</sup> JO L 160 du 18.6.2011, p. 19.

# CHAPITRE I

## DISPOSITIONS GÉNÉRALES

### *Article premier*

#### ***Objet et objectifs***

1. La présente directive établit les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes aux fins de la prévention et de la détection des infractions pénales, d'enquêtes et de poursuites en la matière, de l'exécution de sanctions pénales ou de la protection contre les menaces pour la sécurité publique et de 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 notamment leur droit à la protection des données à caractère personnel; et
- b) veillent à ce que l'échange de données à caractère personnel par les autorités compétentes au sein de l'Union, lorsque cet échange est requis en vertu du droit de l'Union ou du droit national, 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 1<sup>er</sup>, paragraphe 1.

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

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

- a) dans le cadre d'une activité n'entrant pas dans le champ d'application du droit de l'Union (...); (...)
- 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, à un numéro d'identification, à des données de localisation, à des identifiants en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;
- 2) (...)
- 3) "traitement de données à caractère personnel", toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation du traitement, l'effacement ou la destruction;
- 4) "limitation du traitement", le marquage de données à caractère personnel 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 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 par la législation d'un État membre;

- 7) "sous-traitant", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;
- 8) "destinataire", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers; (...) les autorités nationales qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires;
- 9) "violation de données à caractère personnel", une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière;
- 10) "données génétiques", toutes les données (...) 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) (...);
- 12) "données concernant la santé", (...) des données relatives à la santé physique ou mentale d'une personne physique qui révèlent des informations sur l'état de santé de ladite 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 et prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles ou les intérêts, la fiabilité ou le comportement, ou la localisation et les déplacements;
- (...)

14) "autorité compétente", toute autorité publique compétente dans un État membre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou à des fins de protection contre les menaces pour la sécurité publique et de prévention de telles menaces, ou tout organisme/entité à qui la législation nationale confie l'exercice de fonctions publiques ou de prérogatives publiques aux fins (...) énoncées à l'article 1<sup>er</sup>, paragraphe 1 (...);

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, ainsi qu'Interpol.

## 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 licitement *et loyalement*;

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; (...)

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

*e bis*) traitées de manière à leur assurer un niveau de sécurité approprié.

(...)

1 *bis*. (...)

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

(...)

b) le responsable du traitement soit autorisé à traiter ces données pour ces finalités en vertu des dispositions juridiques applicables; et

c) ce traitement soit nécessaire et proportionné à ces autres finalités.

3. Le traitement des données par le même ou un autre responsable du traitement peut inclure (...) l'archivage dans l'intérêt public, (...) le traitement à des fins scientifiques, statistiques ou historiques, pour les finalités énoncées à l'article 1<sup>er</sup>, 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.

#### Article 5

##### ***Distinction entre différentes catégories de personnes concernées***

(...)

#### Article 6

##### ***Vérification de la qualité des données transmises ou mises à disposition***

1. 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, de l'actualité et de la fiabilité desdites données.

2. 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***

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 1<sup>er</sup>, paragraphe 1, **et fondé sur le droit de l'Union ou d'un État membre (...).**

b) (...)

c) (...)

d) (...)

## 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 1<sup>er</sup>, paragraphe 1, ne peuvent être traitées à des fins autres que celles énoncées à l'article 1<sup>er</sup>, 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 de la législation de l'Union.

1 bis. Lorsque les autorités compétentes sont chargées par la législation des États membres d'exécuter des missions pour des finalités autres que celles énoncées à l'article 1<sup>er</sup>, 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 de la législation de l'Union.

1 ter. Les États membres prévoient que, lorsque (...) le droit de l'Union ou le droit national 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.

2 bis. (...)

## Article 8

### **Traitements portant sur des catégories particulières de données à caractère personnel**

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 ou des données concernant la santé ou la vie sexuelle 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 des États membres (...); 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.

#### Article 9

(...) **Décision individuelle automatisée** (...)

(...) 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 des États membres 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.

(...).

1 bis. (...)

### 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 toutes les mesures raisonnables pour fournir toute information visée à l'article 10 bis (...), ainsi que pour procéder à toute communication visée aux articles 12, 15 et 29 en ce qui concerne le traitement des données à caractère personnel de la personne concernée d'une façon compréhensible et facilement 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 prend toutes les mesures raisonnables afin (...) de faciliter l'exercice des droits conférés à la personne concernée en vertu des articles 12 et 15 (...).

4. (...)

5. Les États membres prévoient que les informations visées à l'article 10 bis (...) ainsi que toute communication au titre des articles 12, 15 et 29 sont fournies (...) gratuitement. Lorsque les demandes sont manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif, le responsable du traitement peut refuser de donner suite à la demande. Dans ce 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 présentant la demande visée aux articles (...) 12 et 15, il peut demander la fourniture des informations complémentaires 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 de l'éventuel délégué à la protection des données;
  - b) les finalités du traitement auquel sont destinées les données à caractère personnel;
  - c) (...)
  - d) ~~(...)~~
  - e) le droit d'introduire une réclamation auprès (...) d'une autorité de contrôle (...).
2. Les États membres (...) prévoient, par voie législative, que le responsable du traitement fournit à la personne concernée des informations supplémentaires à celles visées au paragraphe 1, (...) lorsque cela est nécessaire (...) dans un cas précis et afin de permettre à la personne concernée d'exercer ses droits, en particulier (...) lorsque les données sont collectées à l'insu de la personne en question.
3. Les États membres peuvent adopter des mesures législatives prévoyant le retardement ou la limitation de la fourniture des informations à communiquer à la personne concernée en application du paragraphe 2 (...), ou la non-fourniture de ces informations, dès lors et aussi longtemps qu'une mesure de cette nature est nécessaire et proportionnée dans une société démocratique, compte tenu des intérêts légitimes de la personne concernée:
  - a) pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;
  - b) pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière, ou à l'exécution de sanctions pénales;
  - c) pour assurer la sécurité publique;
  - d) pour sauvegarder la sécurité nationale;
  - e) pour garantir les droits et libertés d'autrui.

### Article 11

Informations à fournir lorsque des données sont collectées auprès de la personne concernée

(...)

### Article 11 bis

Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée

(...)

### Article 11 ter

#### Limitations du droit à l'information

(...)

### 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, à intervalles raisonnables et gratuitement, la confirmation que des données la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, le droit d'obtenir l'accès auxdites données ainsi que les informations ci-après, par les moyens appropriés:

- a) les finalités du traitement;
- b) (...)
- 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) (...) la durée envisagée pendant laquelle les données à caractère personnel seront conservées ou les règles applicables 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 d'une autorité de contrôle (...);

- g) la communication des données à caractère personnel en cours de traitement, ainsi que, si nécessaire, toute information disponible sur l'origine de ces données;
- h) (...)
- 1 bis. (...)
- 2. (...)
- 2 bis. (...)

### *Article 13*

#### ***Limitations du droit d'accès***

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

- a) pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;
- b) pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière, ou à l'exécution de sanctions pénales;
- c) pour assurer la sécurité publique;
- d) pour sauvegarder la sécurité nationale;
- e) pour garantir les droits et libertés d'autrui.

2. (...)

3. Dans les situations visées au paragraphe 1 (...), les États membres prévoient que le responsable du traitement informe la personne concernée par écrit de tout refus ou de toute limitation de l'accès aux données, (...) ainsi que des motifs du refus ou de la limitation. (...) La présente disposition ne s'applique pas (...) lorsque la communication de ces informations 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.

Article 14

*Modalités supplémentaires de l'exercice du droit d'accès*

(...)

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. (...) Le traitement de toute donnée à caractère personnel dont l'exactitude est contestée par la personne concernée et dont il ne peut être déterminé si elle est exacte ou non peut faire l'objet d'une limitation.

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, compte tenu des intérêts légitimes de la personne concernée, pour:

- a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;
- b) 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) assurer la sécurité publique;
- d) sauvegarder la sécurité nationale;

e) garantir 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.

3. Les États membres prévoient que, dans les cas visés aux paragraphes 1, 1 bis et 1 ter, 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. (...)

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

2. (...)

3. 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. (...)

### **Article 16**

#### **Droit à l'effacement**

(...)

### **Article 17**

#### **Droits des personnes concernées lors des enquêtes et des procédures pénales**

Les États membres peuvent prévoir que les droits (...) visés aux articles 10 bis, 12 et 15 sont exercés conformément au droit (...) national 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 de la probabilité et de la gravité des risques au regard des droits et des libertés des personnes physiques, le responsable du traitement met en œuvre les mesures appropriées pour garantir que le traitement des données à caractère personnel sera effectué dans le respect des dispositions adoptées en vertu de la présente directive et qu'il doit être en mesure d'en faire la preuve.

1 bis. Lorsque cela est proportionné par rapport aux activités de traitement de données, les mesures visées au paragraphe 1 comprennent la mise en œuvre, par le responsable du traitement, de politiques appropriées en matière de protection des données qui précisent les modalités d'application des règles nationales de protection des données (...) mettant en œuvre la présente directive.

2. (...)

*Article 19*

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

1. Compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre et prenant en considération (...) la nature, la portée, le contexte et les finalités du traitement, ainsi que la probabilité et la gravité du risque présenté par le traitement pour les droits et libertés des personnes physiques, les États membres prévoient que le responsable du traitement applique des mesures (...) techniques et organisationnelles appropriées pour l'activité de traitement menée et ses objectifs, telles que la pseudonymisation, de manière à ce que le traitement soit conforme aux prescriptions fixées par les dispositions adoptées en vertu de la présente directive et assure la protection des droits des personnes concernées.

2. Les États membres prévoient que le responsable du traitement met en œuvre des (...) mesures appropriées, en particulier pour un traitement automatisé, 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.

## 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. Ils définissent de manière transparente (...), par voie d'accord, leurs obligations respectives afin de se conformer aux dispositions adoptées en vertu 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 (...), sauf si et dans la mesure où les obligations respectives des responsables du traitement sont définies par le droit de l'Union ou la législation de l'État membre à laquelle les responsables du traitement sont soumis. (...) 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. (...) Sans préjudice de l'article 17, 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 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 prescriptions fixées par les dispositions adoptées en vertu de la présente directive (...).

1 bis. Les États membres prévoient que le sous-traitant ne recrute pas un autre sous-traitant sans l'accord écrit préalable, spécifique ou général, du responsable du traitement. Dans ce cas, le sous-traitant devrait toujours informer 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 acte juridique au titre du droit de l'Union ou du droit national, comprenant un contrat 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 droits du responsable du traitement et prévoyant notamment que le sous-traitant n'agit que sur instruction du responsable du traitement (...).

3. (...)

Article 22

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

(...)

Article 23

**Registre des catégories d'activités de traitement de données à caractère personnel**

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 et de tout responsable conjoint du traitement (...) (...) et, le cas échéant, 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, en particulier lorsque les destinataires sont établis dans des pays tiers;
- c bis) une description des catégories de données à caractère personnel relatives (...) aux personnes concernées;
- d) le cas échéant, les catégories de transferts de données à caractère personnel vers un *pays tiers ou à une organisation internationale* (...);
- 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 sous-traitant ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit; (...)
- b) le nom et les coordonnées du délégué à la protection des données, le cas échéant;
- c) les catégories de traitements effectués pour le compte de chaque responsable du traitement;
- d) (...)
- e) (...)
- f) 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, ou sous une autre forme non lisible pouvant être convertie en forme lisible.

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. **À moins que cela se révèle impossible ou suppose un effort disproportionné**, 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, l'interconnexion ou l'effacement. Les journaux des opérations de consultation et de communication indiquent: (...) 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.

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

#### Article 25

##### *Coopération avec l'autorité de contrôle*

(...)

#### Article 26

##### *Consultation préalable de l'autorité de contrôle*

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

- a) le traitement vise des catégories particulières de données à caractère personnel mentionnées à l'article 8;
- b) en raison notamment de l'utilisation de nouveaux mécanismes, technologies ou procédures, le type de traitement présente des risques élevés pour les libertés et droits (...) des personnes concernées.

1 bis. (...) Les États membres prennent les mesures nécessaires pour que l'autorité de contrôle soit consultée durant l'élaboration de propositions de mesures législatives ou réglementaires prévoyant le traitement de données à caractère personnel visé au paragraphe 1.

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

3. Les États membres prévoient que, lorsque l'autorité de contrôle est d'avis que le traitement visé au paragraphe 1 n'est pas conforme aux dispositions adoptées en vertu de la présente directive, en particulier lorsque les risques ne sont pas suffisamment identifiés ou atténués, elle doit, dans un délai maximum de six semaines suivant la demande de consultation, conseiller le responsable du traitement de données, par écrit. 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 ou le sous-traitant est informé des raisons du report dans un délai d'un mois à compter de la réception de la demande.

## SECTION 2

### SÉCURITÉ DES DONNÉES

#### *Article 27*

#### *Sécurité des traitements*

1. Compte tenu des techniques disponibles et des coûts liés à la mise en œuvre et prenant en considération la nature, la portée, le contexte et les finalités du traitement ainsi que la probabilité et la gravité du risque pour les droits et libertés des personnes physiques, les États membres prévoient que le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées (...) afin de garantir un niveau de sécurité adapté au risque.

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 du stockage);
- d) empêcher que les systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs);
- e) garantir que les personnes autorisées à utiliser un système de traitement automatisé de données ne puissent accéder qu'aux données sur lesquelles porte leur autorisation (contrôle de l'accès aux données);

- f) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission);
  - g) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé de données, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction);
  - h) empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou 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 susceptible d'exposer les personnes concernées à un risque élevé au regard de leurs droits et libertés (...), 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. Lorsqu'elle a lieu après ce délai de 72 heures, la notification comporte une justification à cet égard.  
1 bis. La notification visée au paragraphe 1 n'est pas requise si une communication à la personne concernée n'est pas nécessaire aux termes de l'article 29, paragraphe 3, points a) et b). (...)
2. Le sous-traitant alerte et informe le responsable du traitement dans les meilleurs délais après avoir eu connaissance de la violation de données à caractère personnel.
3. La notification visée au paragraphe 1 doit, à tout le moins:
  - a) décrire la nature de la violation de données à caractère personnel;
  - b) communiquer l'identité et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;
  - c) (...)
  - d) décrire les conséquences probables de la violation de données à caractère personnel constatée par le responsable du traitement;

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

f) le cas échéant, indiquer des mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données à caractère personnel.

3 bis. Si et dans la mesure où il n'est pas possible de fournir les informations visées au paragraphe 3, points d), e) et f), en même temps que les informations visées au paragraphe 3, points a) et b), le responsable du traitement fournit ces informations sans autre retard.

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. Sous réserve du paragraphe 1 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. Sous réserve des paragraphes 3 et 4 du présent article, les États membres prévoient que, lorsque la violation de données à caractère personnel est susceptible d'exposer la personne concernée à un risque élevé au regard de ses droits et libertés (...), le responsable du traitement (...) communique la violation à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée prévue au paragraphe 1 décrit la nature de la violation des données à caractère personnel et contient au moins les informations visées à l'article 28, paragraphe 3, points b), e) et f).

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 technologiques et organisationnelles appropriées et si ces dernières ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier celles 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 au regard des *droits et des libertés* des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser; ou
- c) elle risque d'entraîner des mesures disproportionnées, eu égard notamment au nombre de cas concernés. 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.

4. La communication à la personne concernée visée au paragraphe 1 peut être retardée, limitée ou omise 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 peuvent prévoir ou, si le *droit de l'Union* (...) l'exige, prévoient que le responsable du traitement ou le sous-traitant désigne un délégué à la protection des données.
2. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées de la législation et des pratiques en matière de protection des données, ainsi que de sa capacité à accomplir les missions énumérées à l'article 32, notamment l'absence de tout conflit d'intérêts.
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.
4. *Les États membres prévoient que le responsable du traitement ou le sous-traitant veille à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.*

5. Le responsable du traitement ou le sous-traitant veille à ce que le délégué à la protection des données soit doté des moyens d'accomplir les missions (...) visées à l'article 32 et puisse agir en toute indépendance dans l'accomplissement de ses missions (...).

#### Article 31

##### **Fonction du délégué à la protection des données**

(...)

#### Article 32

##### **Missions du délégué à la protection des données**

Les États membres prévoient que le responsable du traitement ou le sous-traitant confie au délégué à la protection des données (...) les missions suivantes:

- a) informer et conseiller le responsable du traitement ou le sous-traitant (...) sur les obligations qui leur incombent en application des dispositions adoptées en vertu de la présente directive et d'autres dispositions de l'Union ou de l'État membre concerné en matière de protection des données (...);
- b) contrôler la conformité avec les dispositions adoptées en vertu de la présente directive, avec d'autres dispositions de l'Union ou de l'État membre concerné en matière de protection des données et (...) avec les règles internes du responsable du traitement ou du sous-traitant 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 traitements, et les audits s'y rapportant;
- c) (...)
- d) (...)
- e) (...)
- f) (...)
- g) vérifier qu'il a été répondu aux demandes de l'autorité de contrôle et, dans le domaine de compétence du délégué à la protection des données, coopérer avec l'autorité de contrôle, à la demande de celle-ci ou à l'initiative du délégué à la protection des données;
- h) faire office de point de contact pour l'autorité de contrôle sur les questions liées au traitement 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 (...) vers un pays tiers ou à une organisation internationale, y compris un transfert ultérieur vers un autre pays tiers ou une autre organisation internationale, ne peut avoir lieu que si:
- a) le transfert est nécessaire aux fins énoncées à l'article 1<sup>er</sup>, paragraphe 1; et
  - b) (...)
  - c) le responsable du traitement dans le pays tiers ou l'organisation internationale est une autorité compétente aux fins énoncées à l'article 1<sup>er</sup>, 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 son droit national; 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. (...)
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. Les États membres prévoient qu'en l'absence de décision constatant le caractère adéquat du niveau de protection conformément à l'article 34 ou de garanties appropriées conformément à l'article 35, un transfert ne peut avoir lieu que lorsque des dérogations pour des situations particulières s'appliquent conformément à l'article 36 et que les conditions visées au paragraphe 1, points a), c) et d), et, le cas échéant, (...) au paragraphe 2, sont remplies.

## Article 34

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

1. Les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers, ou un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision, conformément à l'article 41 du règlement (UE) .../XXX ou conformément au paragraphe 3 du présent article, que le pays tiers, le territoire ou le secteur déterminé 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'aucune décision adoptée en vertu de l'article 41 du règlement (UE) .../XXX ne s'applique, la Commission apprécie le caractère adéquat du niveau de protection en tenant 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, les règles en matière de protection des données (...) notamment en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal, et (...) les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une organisation internationale, qui sont respectées dans le pays tiers en question ou par l'organisation internationale en question, ainsi que l'existence de droits des personnes concernées effectifs et opposables et d'un droit de recours administratif et judiciaire effectif des 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, notamment 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 de l'Union et des États membres; et
  - c) les engagements internationaux pris par le pays tiers ou l'organisation internationale concerné, ou d'autres obligations lui incombant en raison de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

- 2 bis. Le comité européen de la protection des données rend 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.
3. La Commission, après avoir évalué le caractère adéquat du niveau de protection, peut constater par voie de décision, dans les limites de la présente directive, 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 précise son champ d'application territorial et sectoriel et, le cas échéant, cite le nom de la ou des autorités de contrôle (indépendantes) 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 contrôle le bon fonctionnement des décisions adoptées en vertu du paragraphe 3 (...).
5. La Commission peut constater par voie de décision, dans les limites de la présente directive, qu'un pays tiers, un territoire ou un secteur déterminé dans ce pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat au sens du paragraphe 2 et peut, si nécessaire, abroger, modifier ou suspendre cette décision sans effet rétroactif. Les (...) actes d'exécution correspondants sont adoptés en conformité avec la procédure d'examen prévue à l'article 57, paragraphe 2, ou, en cas d'extrême urgence, en conformité avec la procédure prévue 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 veillent à ce que, lorsqu'une décision est prise en vertu du paragraphe 5, cette décision (...) soit sans préjudice des transferts de données à caractère personnel vers le pays tiers, ou le territoire ou 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* une liste des pays tiers, des territoires et secteurs déterminés dans un pays tiers et des organisations internationales à l'égard desquels des décisions ont été prises au titre des paragraphes 3 (...) et 5.
8. (...)

#### *Article 35*

##### ***Transferts moyennant des garanties appropriées***

1. (...) En l'absence de décision adoptée en vertu de l'article 34, paragraphe 3, 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. Aux fins de cette évaluation, le responsable du traitement peut tenir compte des accords de coopération existants conclus entre Europol ou Eurojust et des pays tiers qui prévoient un échange de données à caractère personnel.
2. (...)

#### *Article 36*

##### ***Dérogations pour (...) des situations particulières***

1. (...) En l'absence d'une décision constatant le caractère adéquat du niveau de protection conformément à 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 si:
  - a) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne; ou
  - b) le transfert est nécessaire à la sauvegarde des intérêts légitimes de la personne concernée (...) lorsque la législation de l'État membre transférant les données à caractère personnel le prévoit; ou
  - c) le transfert de données est 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 1<sup>er</sup>, 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 1<sup>er</sup>, 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).

*Article 36 bis*

(...)

*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, le droit de l'Union ou la législation nationale peut prévoir que les autorités compétentes peuvent, dans certains cas (...) particuliers, transférer les 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 d'une autorité compétente prévue par le droit de l'Union ou la législation nationale aux fins (...) énoncées à l'article 1<sup>er</sup>, paragraphe 1; et
  - b) (...)
  - c) (...)
  - d) 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.
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. (...)

*Article 37*

*Conditions spécifiques applicables au transfert de données à caractère personnel*

*Article 38*

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

(...)

**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 des dispositions adoptées en vertu de la présente directive.
- 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.
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. (...)
4. (...)

5. (...) Les États membres veillent 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 ceux qu'elle doit mettre en œuvre dans le cadre de l'assistance mutuelle, de la coopération et de la participation active au comité européen de la protection des données.
6. (...) Les États membres veillent à ce que chaque autorité de contrôle dispose de ses propres agents, qui sont (...) placés sous les ordres 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, pouvant faire partie du budget général de l'État ou du budget national.

#### *Article 41*

##### ***Conditions générales applicables aux membres de l'autorité de contrôle***

1. Les États membres prévoient que le membre ou (...) les membres de chaque autorité de contrôle doivent être nommés par le parlement et/ou par le gouvernement ou le chef d'État de l'État membre concerné ou par un organisme indépendant chargé par la législation de l'État membre de procéder à la nomination selon une procédure transparente.
2. Le membre ou les membres ont les qualifications, l'expérience et les compétences nécessaires pour l'exercice de leurs fonctions et de leurs pouvoirs.
3. (...) Les fonctions des membres prennent fin à l'échéance de leur mandat, en cas de démission ou de mise à la retraite d'office, conformément à (...) la législation de l'État membre. (...)
4. (...)
5. (...)

Article 42

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

1. Les États membres prévoient, par voie législative:
- a) la création de chaque autorité de contrôle (...);
  - b) (...) les qualifications (...) requises pour exercer les fonctions de membre de l'autorité de contrôle;
  - c) les règles et les procédures pour la nomination du membre ou des membres de chaque autorité de contrôle (...);
  - d) la durée du mandat du membre ou des membres de chaque autorité de contrôle, qui ne doit pas être 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 ou d'emplois incompatibles avec celles-ci, y compris après la cessation de leurs activités, et les règles régissant la cessation de l'emploi.
  - g) (...)

1 bis. Les États membres prévoient que 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 nationale, au secret professionnel concernant toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs (...) fonctions (...) ou de leurs pouvoirs, y compris après la cessation de leurs activités.

Article 43

***Secret professionnel***

(...)

**SECTION 2**  
**MISSIONS ET POUVOIRS**

*Article 44*

***Compétence***

1. Les États membres prévoient que chaque autorité de contrôle est compétente, sur le territoire de l'État membre dont elle relève, pour accomplir les missions et exercer (...) les pouvoirs dont elle est investie conformément à la présente directive. (...)
2. Les États membres prévoient que l'autorité de contrôle n'est pas compétente pour contrôler les traitements effectués par les (...) juridictions dans l'exercice de leurs fonctions juridictionnelles. 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 leurs fonctions juridictionnelles.

*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 concernées 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 application des dispositions adoptées en vertu de la présente directive;
  - a quinquies) fournit des informations, sur demande, à toute personne concernée sur l'exercice de ses droits découlant des dispositions adoptées en vertu 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 la représentant et dûment mandatée par elle (...), examine l'objet de la réclamation, dans la mesure nécessaire, et informe la personne concernée ou l'organisme, l'organisation ou l'association 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 3, ou des motifs ayant empêché sa réalisation;
  - d) coopère avec d'autres autorités de contrôle, y compris en partageant des informations, et prévoit une assistance mutuelle en vue d'assurer une application cohérente des dispositions adoptées en vertu de la présente directive et des mesures prises pour en assurer le respect;
  - e) effectue des enquêtes sur l'application des dispositions adoptées en vertu 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) surveille les faits nouveaux présentant un intérêt, dans la mesure où ils ont une incidence sur la protection des données à caractère personnel, notamment l'évolution des technologies de l'information et des communications(...);
  - g) (...)
  - h) fournit des conseils sur les traitements visés à l'article 26;
  - i) contribue aux activités du comité européen de la protection des données.
2. (...)
3. (...)
4. (...)
5. Les États membres prévoient que l'accomplissement des missions de chaque autorité de contrôle est gratuit pour la personne concernée et pour le délégué à la protection des données, le cas échéant.
6. Les États membres prévoient que (...) lorsque les demandes sont manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif, l'autorité de contrôle peut refuser de donner suite à la demande. Il incombe à l'autorité de contrôle d'établir 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;

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 traitements envisagés sont susceptibles de violer les dispositions adoptées en vertu de la présente directive;
- b) (...)
- c) (...)
- d) ordonner au responsable du traitement ou au sous-traitant de mettre les traitements 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;
- e) limiter temporairement ou définitivement un traitement;
- f) (...)

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 nationale 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 47*

***Rapport d'activité***

Les États membres prévoient que chaque autorité de contrôle établit un rapport annuel sur son activité. 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 européenne et du comité européen de la protection des données.

## CHAPITRE VII COOPÉRATION

### Article 48

#### *Assistance mutuelle*

1. Les États membres prévoient que les autorités de contrôle se prêtent une assistance mutuelle en vue de mettre en œuvre et d'appliquer (...) les dispositions adoptées en vertu de la présente directive, et qu'elles mettent en place des mesures pour coopérer efficacement entre elles. L'assistance mutuelle couvre notamment des demandes d'information et des mesures de contrôle, telles que les demandes (...) d'inspection et d'enquête.
  2. Les États membres prévoient qu'une autorité de contrôle prend toutes les mesures appropriées requises pour répondre à la demande d'une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande. (...)
- (...)
- 2 ter. Les États membres prévoient qu'une autorité de contrôle saisie d'une demande d'assistance ne peut refuser d'y donner suite, à moins:
- a) qu'elle ne soit pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter; ou
  - b) que le fait de satisfaire à la demande soit incompatible avec les dispositions adoptées en vertu 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. Les autorités de contrôle communiquent en règle générale par des moyens électroniques 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 objet du 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 conformément à 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 des dispositions adoptées en vertu de la présente directive, et publier des lignes directrices, des recommandations et des bonnes pratiques (...), afin de favoriser l'application cohérente de ces dispositions;
  - 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 (...);
  - c) faire le bilan de l'application pratique des lignes directrices, recommandations et bonnes pratiques visées aux points b) et b bis) (...);
  - d) communiquer à la Commission un avis sur le niveau de protection assuré dans des pays tiers ou des organisations internationales;
  - e) promouvoir la coopération et l'échange bilatéral et multilatéral effectif d'informations et de pratiques entre les autorités de contrôle;
  - f) promouvoir l'élaboration de programmes de formation conjoints et faciliter les échanges de personnel entre autorités de contrôle, ainsi que, le cas échéant, avec les autorités de contrôle de pays tiers ou d'organisations internationales;
  - g) promouvoir l'échange, avec des autorités de contrôle de la protection des données de tous pays, de connaissances et de documentation *sur la législation et les pratiques en matière de protection des données.*
2. Lorsque la Commission consulte le comité européen de la protection des données, elle peut 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 il les publie.
4. La Commission informe le comité européen de la protection des données de la suite qu'elle a réservée aux avis, lignes directrices, recommandations et bonnes pratiques 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 conformément à 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, chaque personne concernée a le droit de former un recours juridictionnel effectif lorsque l'autorité de contrôle compétente en vertu de l'article 44, paragraphe 1, ne traite pas une réclamation (...) ou n'informe pas la personne concernée dans un délai de trois mois, ou dans un délai plus court prévu par le droit de l'Union ou la législation nationale, 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 effectif 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 de saisir une autorité de contrôle d'une réclamation conformément à l'article 50, les personnes concernées disposent d'un recours juridictionnel effectif si elles considèrent qu'il a été porté atteinte aux droits que leur confèrent les dispositions adoptées conformément à la présente directive, à la suite d'un traitement de données à caractère personnel les concernant effectué en violation de ces 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(e) conformément au droit d'un État membre et dont les objectifs statutaires comprennent la protection des droits et des libertés des personnes concernées à l'égard de la protection de leurs données à caractère personnel, pour qu'il ou elle introduise une réclamation en son nom et exerce en son nom les droits prévus 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 (...) du fait (...) d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de (...) la présente directive a le droit d'obtenir du responsable du traitement, ou de toute autre autorité compétente en vertu du droit national, réparation du préjudice subi (...).
2. (...)
3. (...)
4. (...)
5. (...)

## Article 55

### ***Sanctions***

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

**CHAPITRE IX**  
**(...) ACTES D'EXÉCUTION**

*Article 56*

***Exercice de la délégation***

(...)

*Article 57*

***Procédure de comité***

1. La Commission est assistée par le comité institué par l'article 87 du règlement (UE) .../XXX. Ce comité est un comité au sens du règlement (UE) n° 182/2011.
2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 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 aux dispositions du droit de l'Union applicables 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 évalue l'application de la présente directive. Dans le cadre de cette évaluation, la Commission examine, en particulier, l'application et le fonctionnement des dispositions de l'article 36 bis bis.

2. Dans un délai de cinq 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 1<sup>er</sup>, paragraphe 1, y compris les actes adoptés par l'Union qui sont mentionnés à l'article 59, afin d'apprécier la nécessité de les mettre en conformité avec la présente directive et de formuler, le cas échéant, les propositions nécessaires en vue de modifier ces actes pour assurer une approche cohérente de la protection des données à caractère personnel dans le cadre de la présente directive.
3. La Commission présente périodiquement des rapports sur l'évaluation et la révision de la présente directive au Parlement européen et au Conseil, conformément au paragraphe 1. Le premier rapport est présenté au plus tard quatre ans après l'entrée en vigueur de la présente directive. Les rapports suivants sont ensuite présentés tous les quatre ans. La Commission soumet, si nécessaire, les propositions ad hoc pour modifier la présente directive et harmoniser d'autres instruments juridiques. Le rapport est publié.

#### *Article 62*

#### ***Transposition***

1. Les États membres adoptent et publient, au plus tard le [date/trois 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/trois ans après l'entrée en vigueur]. Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.
2. Les États membres communiquent à la Commission le texte des 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.

---