DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 27 avril 2016

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, et abrogeant la décision-cadre 2008/977/JAI du Conseil

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

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

vu la proposition de la Commission européenne,

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

vu l'avis du Comité des régions [1],

statuant conformément à la procédure législative ordinaire [2],

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 (ci-après dénommée «Charte») 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 applicables en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel. La présente directive vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice.

(3) L'évolution rapide des technologies et la mondialisation ont créé de nouveaux défis pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent de traiter 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) Il convient de faciliter le libre flux des données à caractère personnel entre les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces au sein de l'Union, et le transfert de telles données vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel. Ces évolutions obligent à mettre en place dans l'Union un cadre pour la protection des données à caractère personnel solide et plus cohérent, assorti d'une application rigoureuse des règles.

(5) La directive 95/46/CE du Parlement européen et du Conseil [3] s'applique à l'ensemble des traitements des données à caractère personnel dans les États membres, à la fois dans le

secteur public et le secteur privé. Elle ne s'applique cependant pas au traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que les activités dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière.

(6) La décision-cadre 2008/977/JAI du Conseil [4] s'applique dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière. Son champ d'application se limite au traitement des données à caractère personnel qui sont transmises ou mises à disposition entre les États membres.

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

(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 et les règles relatives à la libre circulation de ces données.

(9) Sur cette base, le règlement (UE) 2016/679 du Parlement européen et du Conseil [5] 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.

(10) Dans la déclaration n° 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 des données à caractère personnel 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) Il convient dès lors que ces domaines soient régis par une directive qui fixe les règles spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, en respectant la nature spécifique de ces activités. Les autorités compétentes en question peuvent comprendre non seulement les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais aussi tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la présente directive. Lorsqu'un tel organisme ou une telle entité traite des données à caractère

personnel à des fins autres que celles prévues dans la présente directive, le règlement (UE) 2016/679 s'applique. Par conséquent, le règlement (UE) 2016/679 s'applique lorsqu'un organisme ou une entité recueille des données à caractère personnel à d'autres fins et les traite ultérieurement pour respecter une obligation légale à laquelle il est soumis. Par exemple, les établissements financiers conservent, à des fins de détection ou de poursuites d'infractions pénales ou d'enquêtes en la matière, certaines données à caractère personnel qu'ils traitent et qu'ils ne transmettent aux autorités nationales compétentes que dans des cas spécifiques et conformément au droit des États membres. Un organisme ou une entité qui traite des données à caractère personnel pour le compte de ces autorités dans le cadre du champ d'application de la présente directive devrait être lié par un contrat ou un autre acte juridique et par les dispositions applicables aux sous-traitants en vertu de la présente directive, le règlement (UE) 2016/679 continuant de s'appliquer aux traitements de données à caractère personnel par le sous-traitant en dehors du champ d'application de la présente directive.

(12)Les activités menées par la police ou d'autres autorités répressives sont axées principalement sur la prévention et la détection des infractions pénales et les enquêtes et les poursuites en la matière, y compris les activités de police effectuées sans savoir au préalable si un incident constitue une infraction pénale ou non. Ces activités peuvent également comprendre l'exercice de l'autorité par l'adoption de mesures coercitives, par exemple les activités de police lors de manifestations, de grands événements sportifs et d'émeutes. Parmi ces activités figure également le maintien de l'ordre public lorsque cette mission est confiée à la police ou à d'autres autorités répressives lorsque cela est nécessaire à des fins de protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la société protégés par la loi, et de prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale. Les États membres peuvent confier aux autorités compétentes d'autres missions qui ne sont pas nécessairement menées à des fins de prévention et de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, de sorte que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application du droit de l'Union, relève du champ d'application du règlement (UE) 2016/679.

(13)La notion d'infraction pénale au sens de la présente directive devrait être une notion autonome du droit de l'Union conforme à l'interprétation de la Cour de justice de l'Union européenne (ci-après dénommée «Cour de justice»).

(14)Étant donné que la présente directive ne devrait pas s'appliquer au traitement de données à caractère personnel effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union, il convient que les activités relatives à la sécurité nationale, les activités des agences ou des services responsables des questions de 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 considérées comme des activités relevant du champ d'application de la présente directive.

(15)Afin d'assurer le même niveau de protection pour les personnes physiques à l'aide de droits opposables dans l'ensemble de l'Union et d'éviter que des divergences n'entravent les échanges de données à caractère personnel entre les autorités compétentes, la présente directive devrait prévoir des règles harmonisées pour la protection et la libre circulation des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la

prévention de telles menaces. Le rapprochement des législations des États membres ne devrait pas conduire à un affaiblissement de la protection des données à caractère personnel qu'elles offrent 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 étendues que celles établies dans 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.

(16) La présente directive s'applique sans préjudice du principe du droit d'accès du public aux documents officiels. En vertu du règlement (UE) 2016/679, les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique ou par un organisme public ou privé pour l'exécution d'une mission d'intérêt public peuvent être communiquées par cette autorité ou cet organisme conformément au droit de l'Union ou au droit de l'État membre auquel l'autorité publique ou l'organisme public est soumis, afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel.

(17) La protection conférée par la présente directive devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel.

(18) Afin d'éviter de créer un risque grave de contournement, la protection des personnes physiques devrait être neutre sur le plan technologique et ne devrait pas dépendre des techniques utilisées. Elle devrait s'appliquer aux traitements de données à caractère personnel à l'aide de procédés automatisés ainsi qu'aux traitements manuels, si les données à caractère personnel 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.

(19) Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil (6) s'applique au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union. Le règlement (CE) n° 45/2001 et les autres actes juridiques de l'Union applicables audit traitement des données à caractère personnel devraient être adaptés aux principes et aux règles fixés dans le règlement (UE) 2016/679.

(20) La présente directive n'empêche pas les États membres de préciser, dans les règles nationales relatives aux procédures pénales, les opérations et les procédures de traitement en ce qui concerne le traitement des données à caractère personnel par les juridictions et les autres autorités judiciaires, notamment pour ce qui est des données à caractère personnel figurant dans les décisions judiciaires ou les documents relatifs aux procédures pénales.

(21) Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une

personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable.

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

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

(24) Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil (7) au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, des antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro.

(25) Tous les États membres sont affiliés à l'Organisation internationale de police criminelle (Interpol). Pour exécuter sa mission, Interpol reçoit, conserve et diffuse des données à caractère personnel pour aider les autorités compétentes à prévenir et à combattre la criminalité internationale. Il est dès lors approprié de renforcer la coopération entre l'Union et Interpol en favorisant un échange efficace de données à caractère personnel tout en garantissant le respect des libertés et droits fondamentaux en ce qui concerne le traitement automatique des données à caractère personnel. Lorsque des données à caractère personnel sont transférées de l'Union vers Interpol, et vers des pays qui ont délégué des membres à

Interpol, la présente directive, en particulier ses dispositions relatives aux transferts internationaux, devrait s'appliquer. La présente directive devrait être sans préjudice des règles spécifiques énoncées dans la position commune 2005/69/JAI du Conseil [(8)] et dans la décision 2007/533/JAI du Conseil [(9)].

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

(27)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 cadre de la prévention et de la détection d'infractions pénales spécifiques, et des enquêtes et poursuites en la matière au-delà de ce cadre, pour acquérir une meilleure compréhension des activités criminelles et établir des liens entre les différentes infractions pénales mises au jour.

(28)Afin de préserver la sécurité entourant le traitement et de prévenir tout traitement effectué en violation de la présente directive, il convient que les données à caractère personnel soient traitées de manière à garantir un niveau de sécurité et de confidentialité approprié, notamment en empêchant 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, et à tenir compte de l'état des connaissances et de la technologie disponible, des coûts de mise en œuvre au regard des risques et de la nature des données à caractère personnel à protéger.

(29)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 les finalités de prévention et de

détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, y compris de protection contre les menaces pour la sécurité publique et de prévention de telles menaces. Si des données à caractère personnel sont traitées par le même responsable du traitement ou un autre pour une finalité relevant du champ d'application de la présente directive autre que celle pour laquelle elles ont été collectées, un tel traitement devrait être permis à condition qu'il soit autorisé conformément aux dispositions légales applicables et qu'il soit nécessaire et proportionné au regard de cette autre finalité.

(30)Il convient d'appliquer le principe d'exactitude des données tout en tenant compte de la nature et de la finalité du traitement concerné. Dans le cadre des procédures judiciaires notamment, les déclarations contenant des données à caractère personnel sont fondées sur les perceptions subjectives des personnes physiques et ne sont pas toujours vérifiables. Le principe d'exactitude ne devrait, par conséquent, pas s'appliquer à l'exactitude de la déclaration elle-même mais simplement au fait qu'une déclaration déterminée a été faite.

(31)Le traitement des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière implique nécessairement le traitement de données à caractère personnel concernant différentes catégories de personnes concernées. Il importe dès lors d'établir une distinction claire, le cas échéant et dans la mesure du possible, entre les données à caractère personnel de différentes catégories de personnes concernées, telles que: les suspects; les personnes reconnues coupables d'une infraction pénale; les victimes et les autres parties, tels que les témoins; les personnes détenant des informations ou des contacts utiles; et les complices de personnes soupçonnées et de criminels condamnés. Cela ne devrait pas empêcher l'application du droit à la présomption d'innocence garanti par la Charte et par la convention européenne des droits de l'homme, telles qu'elles ont été interprétées respectivement par la Cour de justice et par la Cour européenne des droits de l'homme dans leur jurisprudence.

(32)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 la protection des personnes physiques, l'exactitude, et la fiabilité des données à caractère personnel transmises ou mises à disposition ainsi que leur exhaustivité ou leur niveau de mise à jour, les autorités compétentes devraient, dans la mesure du possible, ajouter les informations nécessaires dans tous les transferts de données à caractère personnel.

(33)Lorsque la présente directive fait référence au droit d'un État membre, à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné. Cependant, ce droit d'un État membre, cette base juridique ou cette mesure législative devrait être clair et précis et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice et de la Cour européenne des droits de l'homme. Le droit des États membres qui réglemente le traitement des données à caractère personnel relevant du champ d'application de la présente directive devrait préciser au minimum les objectifs, les données à caractère personnel qui feront l'objet d'un traitement, les finalités du traitement et les procédures pour garantir l'intégrité et la confidentialité des données à caractère personnel et les procédures prévues pour la destruction de celles-ci, fournissant ainsi des garanties suffisantes vis-à-vis des risques d'utilisation abusive et d'arbitraire.

(34)Le traitement de données à caractère personnel effectué par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la

matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, devrait couvrir les opérations ou séries d'opérations appliquées à des données ou à des ensembles de données à caractère personnel à ces fins, qu'elles soient effectuées à l'aide de procédés automatisés ou d'une autre manière, 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 une autorité compétente communique de manière licite les données à caractère personnel. Lorsque des données à caractère personnel ont été initialement collectées par une autorité compétente pour l'une des finalités prévues par la présente directive, le règlement (UE) 2016/679 devrait s'appliquer au traitement de ces données à des fins autres que celles prévues par la présente directive lorsqu'un tel traitement est autorisé par le droit de l'Union ou le droit d'un État membre. En particulier, les règles fixées dans le règlement (UE) 2016/679 devraient s'appliquer au transfert de données à caractère personnel à des fins ne relevant pas du champ d'application de la présente directive. Le règlement (UE) 2016/679 devrait s'appliquer au traitement de données à caractère personnel par un destinataire qui n'est pas une autorité compétente ou qui n'agit pas en cette qualité au sens de la présente directive et auquel une autorité compétente communique de manière licite des données à caractère personnel. Dans le cadre de la mise en œuvre de la présente directive, les États membres devraient aussi pouvoir préciser plus en détail les modalités d'application des règles du règlement (UE) 2016/679, sous réserve des conditions fixées dans ledit règlement.

(35) Pour être licite, le traitement des données à caractère personnel au titre de 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 le droit d'un État membre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Ces activités devraient couvrir la protection des intérêts vitaux de la personne concernée. Dans le cadre de l'exécution des missions de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales qui leur sont confiées de manière institutionnelle par la loi, les autorités compétentes peuvent demander ou ordonner aux personnes physiques de donner suite aux demandes qui leur sont adressées. Dans ce cas, le consentement de la personne concernée, au sens du règlement (UE) 2016/679, ne devrait pas constituer une base juridique pour le traitement de données à caractère personnel par les autorités compétentes. Lorsqu'elle est tenue de respecter une obligation légale, la personne concernée ne dispose pas d'une véritable liberté de choix; sa réaction ne pourrait dès lors être considérée comme une manifestation libre de sa volonté. Cela ne devrait pas empêcher les États membres de prévoir par la loi 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.

(36) Les États membres devraient prévoir que lorsque le droit de l'Union ou le droit d'un État membre applicable à l'autorité compétente qui transmet les données soumet le traitement de données à caractère personnel à des conditions spécifiques applicables dans certaines

situations particulières, telles que l'utilisation de codes de traitement, l'autorité compétente qui transmet les données devrait informer le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter. Ces conditions pourraient, par exemple, comprendre une interdiction de transmission ultérieure des données à caractère personnel à autrui, une interdiction d'utilisation desdites données à des fins autres que celles pour lesquelles elles ont été transmises au destinataire, ou une interdiction d'informer la personne concernée lorsque le droit à l'information est limité en l'absence d'autorisation préalable de l'autorité compétente qui transmet les données. Ces obligations devraient également s'appliquer aux transferts de données par l'autorité compétente qui transmet les données à des destinataires dans des pays tiers ou des organisations internationales. Les États membres devraient veiller à ce que l'autorité compétente qui transmet les données n'applique pas aux destinataires dans les autres États membres ou aux services, organes et organismes établis en vertu du titre V, chapitres 4 et 5, 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 dont relève ladite autorité compétente.

(37) Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits. Ces données à caractère personnel devraient comprendre les 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 adhère à des théories tendant à établir l'existence de races humaines distinctes. Ces données à caractère personnel ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne s'accompagne de garanties appropriées pour les droits et libertés de la personne concernée fixées par la loi et ne soit permis dans des cas autorisés par la loi; lorsqu'il n'est pas déjà autorisé par une telle loi, qu'il ne soit nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne; ou qu'il ne porte sur des données manifestement rendues publiques par la personne concernée. Des garanties appropriées pour les droits et des libertés de la personne concernée pourraient comprendre la possibilité de ne collecter ces données qu'en rapport avec d'autres données relatives à la personne physique concernée, la possibilité de sécuriser les données collectées de manière adéquate, des règles plus strictes pour l'accès du personnel de l'autorité compétente aux données et l'interdiction de la transmission de ces données. Il convient également que le traitement de pareilles données soit autorisé par la loi lorsque la personne concernée a expressément marqué son accord au traitement qui est particulièrement intrusif pour elle. Toutefois, l'accord de la personne concernée ne devrait pas constituer en soi une base juridique pour le traitement de ces données à caractère personnel sensibles par les autorités compétentes.

(38) 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 est prise sur le seul fondement d'un traitement automatisé et qui produit des effets juridiques défavorables la concernant ou qui l'affecte de manière significative. En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, y compris la fourniture d'informations spécifiques à la personne concernée et le droit d'obtenir une intervention humaine, en particulier d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision. Tout profilage qui entraîne une discrimination à l'égard de personnes physiques sur la base de données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des

droits fondamentaux, devrait être interdit en application des conditions établies aux articles 21 et 52 de la Charte.

(39)Afin de permettre aux personnes concernées d'exercer leurs droits, toute information qui leur est communiquée devrait être aisément accessible, y compris sur le site internet du responsable du traitement, et facile à comprendre, et formulée en des termes clairs et simples. Ces informations devraient être adaptées aux besoins des personnes vulnérables telles que les enfants.

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

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

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

(43)Une personne physique devrait avoir le droit d'accéder aux données qui ont été collectées la concernant et d'exercer ce droit facilement, à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité. En conséquence, chaque personne concernée devrait avoir le droit de connaître et de se faire communiquer les finalités du traitement des données, la durée pendant laquelle les données sont traitées, ainsi que l'identité des destinataires, y compris les destinataires se trouvant dans des pays tiers. Lorsque ces communications comportent des informations relatives à l'origine des données à caractère personnel, ces informations ne devraient pas révéler l'identité des personnes physiques, en particulier les sources confidentielles. Pour que ce droit soit respecté, il suffit que la personne concernée dispose d'un aperçu complet de ces données sous une forme intelligible, c'est-à-dire une forme qui lui permette de prendre connaissance de ces données et de vérifier si elles sont exactes et traitées conformément à la présente directive, de sorte

qu'elle puisse exercer les droits que lui confère la présente directive. Cet aperçu pourrait être fourni sous la forme d'une copie des données à caractère personnel faisant l'objet du traitement.

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

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

(46) Toute limitation des droits de la personne concernée doit respecter la Charte et la convention européenne des droits de l'homme, telles qu'elles sont interprétées respectivement par la Cour de justice et par la Cour européenne des droits de l'homme dans leur jurisprudence, et notamment respecter l'essence desdits droits et libertés.

(47) Une personne physique devrait avoir le droit de faire rectifier des données à caractère personnel inexactes la concernant, en particulier lorsque cela touche aux faits, et disposer d'un droit d'effacement lorsque le traitement de ces données constitue une violation de la présente directive. Cependant, le droit de rectification ne devrait pas affecter, par exemple, la teneur d'une déposition. Une personne physique devrait également avoir le droit d'obtenir la limitation du traitement lorsqu'elle conteste l'exactitude des données à caractère personnel et qu'il ne peut être déterminé si ces données sont exactes ou non, ou lorsque les données à caractère personnel doivent être conservées à des fins probatoires. Plus particulièrement, les données à caractère personnel devraient faire l'objet d'une limitation du traitement plutôt qu'être effacées si, dans un cas déterminé, 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'une limitation du traitement 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 archivistiques, ou à rendre les données sélectionnées inaccessibles. Dans les fichiers automatisés, la limitation du traitement 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 claire dans le fichier. Cette rectification ou cet effacement des données à caractère personnel ou cette limitation du traitement devraient être communiqués aux destinataires auxquels les données ont été communiquées et aux autorités compétentes à l'origine des données inexactes. Les responsables du traitement devraient également cesser de continuer à diffuser ces données.

(48) Lorsque le responsable du traitement refuse à une personne concernée le droit à l'information, le droit d'accès aux données à caractère personnel, de rectification ou d'effacement de celles-ci ou le droit de limitation du traitement, la personne concernée

devrait avoir le droit de demander à l'autorité de contrôle nationale de vérifier la licéité du traitement. La personne concernée devrait être informée de ce droit. Lorsque l'autorité de contrôle agit au nom de la personne concernée, cette dernière devrait à tout le moins être informée par l'autorité de contrôle que toutes les vérifications ou tous les examens nécessaires par l'autorité compétente ont eu lieu. L'autorité de contrôle devrait également informer la personne concernée de son droit de former un recours juridictionnel.

(49)Lorsque les données à caractère personnel sont traitées dans le cadre d'une enquête pénale ou d'une procédure judiciaire en matière pénale, les États membres devraient pouvoir prévoir que le droit à l'information, le droit d'accès aux données à caractère personnel, de rectification ou d'effacement de celles-ci, et le droit de limitation du traitement sont exercés conformément aux règles nationales relatives à la procédure judiciaire.

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

(51)Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données qui pourraient entraîner des dommages physiques matériels ou un préjudice moral, 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; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur 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 ou l'appartenance syndicale; lorsque des données génétiques ou biométriques sont traitées afin d'identifier une personne de manière unique ou lorsque des données concernant la santé ou des données concernant la vie sexuelle et l'orientation sexuelle, ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes sont traitées; lorsque des aspects personnels sont évalués, en particulier dans le cadre de l'analyse et de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.

(52)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. 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.

(53)La protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel exige l'adoption de mesures techniques et organisationnelles appropriées, pour garantir que les exigences de la présente directive soient respectées. La mise en œuvre de telles mesures ne devrait pas dépendre uniquement de considérations économiques. Afin d'être en mesure de démontrer qu'il respecte la présente directive, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut. Lorsque le responsable du traitement a procédé à une analyse d'impact relative à la protection des données en vertu de la présente directive, les résultats devraient être pris en compte lors de l'élaboration desdites mesures et procédures. Les mesures pourraient consister notamment dans le recours à la pseudonymisation le plus tôt possible. Le recours à la pseudonymisation aux fins de la présente directive peut servir d'outil susceptible de faciliter, en particulier, le libre flux des données à caractère personnel au sein de l'espace de liberté, de sécurité et de justice.

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

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

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

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

(58)Lorsque des opérations de traitement sont, du fait de leur nature, de leur portée ou de leurs finalités, susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement devrait effectuer une analyse d'impact relative à

la protection des données comprenant notamment les mesures, les garanties et les mécanismes envisagés pour assurer la protection des données à caractère personnel et pour apporter la preuve du respect de la présente directive. Les analyses d'impact devraient porter sur les systèmes et processus pertinents des opérations de traitement, et non sur des cas individuels.

(59) 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 préalablement au traitement.

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

(61) 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 un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important pour la personne physique concernée. En conséquence, dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il convient qu'il notifie cette violation de données à caractère personnel à l'autorité de contrôle dans les meilleurs délais et, lorsque c'est possible, dans les 72 heures au plus tard après en avoir pris connaissance, à moins qu'il ne puisse démontrer, conformément au principe de responsabilité, qu'il est peu probable que la violation en question engendre un risque pour les droits et les libertés des personnes physiques. Si une telle notification ne peut avoir lieu dans ce délai de 72 heures, la notification devrait être assortie des motifs du retard et des informations peuvent être fournies de manière échelonnée sans autre retard indu.

(62) Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, celle-ci devrait être informée dans les meilleurs délais afin qu'elle puisse prendre les précautions qui s'imposent. La communication devrait décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels. Il convient que de telles communications aux personnes physiques concernées soient effectuées aussi rapidement qu'il est raisonnablement possible et en coopération étroite avec l'autorité de contrôle, dans le respect des directives données par celle-ci ou par d'autres autorités compétentes. Par exemple, la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux

personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données ou la survenance de violations similaires peut justifier un délai plus long pour la communication. Lorsque le fait de retarder ou de limiter la communication à la personne physique concernée d'une violation des données à caractère personnel ne permet pas d'éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, d'éviter de nuire à la prévention et à la détection des infractions pénales, aux enquêtes et poursuites en la matière ou à l'exécution de sanctions pénales, de sauvegarder la sécurité publique ou la sécurité nationale, ou de protéger les droits et libertés d'autrui, la communication pourrait, dans des circonstances exceptionnelles, être omise.

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

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

traitement ou à des sous-traitants dans le même pays tiers ou dans un pays tiers différent, ou à une autre organisation internationale.

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

(66)La Commission devrait pouvoir 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, assurant ainsi une sécurité juridique et une uniformité dans l'ensemble de l'Union en ce qui concerne les pays tiers ou les organisations internationales qui sont réputés offrir un tel niveau de protection. Dans ces cas, les transferts de données à caractère personnel vers ces pays devraient pouvoir avoir lieu sans qu'il soit nécessaire d'obtenir une autorisation spécifique, sauf lorsqu'un autre État membre auprès duquel les données ont été collectées doit autoriser le transfert.

(67)Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait, dans son évaluation d'un pays tiers ou d'un territoire ou d'un secteur déterminé dans un pays tiers, prendre en considération la manière dont un pays tiers en particulier respecte l'état de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, y compris la législation sur la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal. Lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision d'adéquation, il y a lieu de prendre en compte des critères clairs et objectifs, telles que les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et du droit en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties assurant un niveau adéquat de protection essentiellement équivalent à celui qui est assuré au sein de l'Union, en particulier lorsque les données sont traitées dans un ou plusieurs secteurs spécifiques. Plus particulièrement, le pays tiers devrait assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération

avec les autorités de protection des données des États membres, et les personnes concernées devraient se voir octroyer des droits effectifs et opposables ainsi que des possibilités effectives de recours administratif ou juridictionnel.

(68) Outre les engagements internationaux pris par le pays tiers ou l'organisation internationale, la Commission devrait également tenir compte des obligations découlant de la participation du pays tiers ou de l'organisation internationale à des systèmes multilatéraux ou régionaux, notamment en matière de protection des données à caractère personnel, ainsi que de la mise en œuvre de ces obligations. Il y a lieu, en particulier, de prendre en considération l'adhésion du pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel. Aux fins de l'évaluation du niveau de protection offert par des pays tiers ou des organisations internationales, la Commission devrait consulter le comité européen de la protection des données établi par le règlement (UE) 2016/679 (ci-après dénommé «comité»). La Commission devrait également tenir compte de toute décision d'adéquation pertinente qu'elle aurait adoptée conformément à l'article 45 du règlement (UE) 2016/679.

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

(70) 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. En conséquence, le transfert de données à caractère personnel vers ce pays tiers ou à cette organisation internationale devrait être interdit, à moins que les exigences de la présente directive relatives aux transferts moyennant des garanties appropriées et aux dérogations pour des situations particulières soient respectées. Il y aurait lieu de prévoir des procédures de consultation entre la Commission et le pays tiers ou l'organisation internationale en question. La Commission devrait informer en temps utile le pays tiers ou l'organisation internationale des motifs de sa conclusion et engager des consultations en vue de remédier à la situation.

(71) Les transferts qui ne sont pas fondés sur une décision d'adéquation 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. Ces instruments juridiquement contraignants pourraient, par exemple, être des accords bilatéraux juridiquement contraignants que les États membres ont conclus et mis en œuvre dans leur ordre juridique et que les personnes concernées pourraient faire exécuter, qui respectent les exigences en matière de protection des données et les droits des personnes concernées, y compris le droit à un recours administratif ou juridictionnel effectif. Lorsqu'il évalue toutes les circonstances entourant le transfert de données, le responsable du traitement devrait pouvoir tenir compte des accords de coopération conclus entre Europol ou Eurojust et des pays tiers qui permettent un échange de données à caractère personnel. Le responsable du traitement devrait aussi pouvoir 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 devrait pouvoir exiger des garanties supplémentaires.

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

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

(74) Lorsque des données à caractère personnel franchissent les frontières, cela peut accroître le risque que les personnes physiques ne puissent exercer leur droit à la protection des données

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

(75) L'institution d'autorités de contrôle dans les États membres, qui sont en mesure d'exercer 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 son application soit cohérente dans l'ensemble de l'Union, afin de protéger les personnes physiques à l'égard du traitement de leurs données à caractère personnel. À cet effet, les autorités de contrôle devraient coopérer entre elles et avec la Commission.

(76) Les États membres peuvent confier à une autorité de contrôle déjà créée en vertu du règlement (UE) 2016/679 la responsabilité des missions incombant aux autorités de contrôle nationales à instituer au titre de la présente directive.

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

(78) 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.

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

(80) Bien que la présente directive s'applique également aux activités des juridictions nationales et autres autorités judiciaires, la compétence des autorités de contrôle ne devrait pas s'étendre au traitement des données à caractère personnel effectué par les juridictions dans l'exercice de leur fonction juridictionnelle, afin de préserver l'indépendance des juges dans l'accomplissement de leurs missions judiciaires. Il convient que cette exception soit limitée aux activités judiciaires 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 conformément au droit d'un État membre. Les États membres devraient aussi pouvoir prévoir que la compétence de l'autorité de contrôle ne s'étend pas aux traitements de données à caractère personnel effectués par d'autres autorités judiciaires indépendantes dans l'exercice de leur fonction juridictionnelle, par exemple le ministère public. En tout état de cause, le respect des règles de la présente directive par les juridictions et autres autorités judiciaires indépendantes fait toujours l'objet d'un contrôle indépendant conformément à l'article 8, paragraphe 3, de la Charte.

(81) Chaque autorité de contrôle devrait traiter les réclamations introduites par les personnes concernées et enquêter sur les affaires en question ou les transmettre à l'autorité de contrôle compétente. L'enquête faisant suite à une réclamation devrait être menée, sous contrôle juridictionnel, dans la mesure appropriée requise par le cas d'espèce. 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.

(82) Afin d'assurer l'efficacité, la fiabilité et la cohérence du contrôle du respect et de l'application de la présente directive dans l'ensemble de l'Union conformément au traité sur le fonctionnement de l'Union européenne tel qu'il est interprété par la Cour de justice, les autorités de contrôle devraient avoir, dans chaque État membre, les mêmes missions et les mêmes pouvoirs effectifs, dont celui d'enquêter, d'adopter des mesures correctrices et d'émettre des avis consultatifs, qui constituent les moyens nécessaires à l'accomplissement de leurs missions. Cependant, leurs pouvoirs ne devraient pas interférer avec les règles spécifiques relatives à la procédure pénale, y compris pour les enquêtes et les poursuites concernant les infractions pénales, ni avec l'indépendance du pouvoir judiciaire. Sans préjudice des pouvoirs des autorités chargées des poursuites en vertu du droit de l'État membre, les autorités de contrôle devraient aussi avoir le pouvoir de porter les violations de la présente directive à l'attention des autorités judiciaires 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 le droit des États membres, d'une manière impartiale et équitable et dans un délai raisonnable. Cela signifie, en particulier, 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 ne soit prise toute mesure individuelle susceptible d'affecter défavorablement la personne concernée et éviter les coûts superflus ainsi que les désagréments excessifs pour la personne concernée. Les pouvoirs d'enquête en ce qui concerne l'accès aux installations devraient être exercés dans le respect des exigences spécifiques du droit de l'État membre, 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 a adopté cette décision.

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

(84) Le comité devrait contribuer à l'application cohérente de la présente directive dans l'ensemble de l'Union, notamment en conseillant la Commission et en favorisant la coopération des autorités de contrôle dans l'ensemble de l'Union.

(85)Toute personne concernée devrait avoir le droit d'introduire une réclamation auprès d'une autorité de contrôle unique et disposer du droit à un recours juridictionnel effectif conformément à l'article 47 de la Charte lorsqu'elle estime qu'il y a violation des droits que lui confèrent les dispositions adoptées en vertu de la présente directive, ou si l'autorité de contrôle ne donne pas à la suite de sa réclamation, la refuse ou la rejette, en tout ou en partie, ou si elle n'agit pas alors qu'une action est nécessaire pour protéger les droits de la personne concernée. L'enquête faisant suite à une réclamation devrait être menée, sous contrôle juridictionnel, dans la mesure appropriée au cas d'espèce. 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 ne soient exclus.

(86)Toute personne physique ou morale devrait disposer du droit à un 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, du pouvoir d'adopter des mesures correctrices et du pouvoir d'autorisation ou le refus ou le rejet de réclamations. Toutefois, ce droit ne couvre pas d'autres mesures prises par les autorités de contrôle qui ne sont pas juridiquement contraignantes, telles que les avis émis ou les conseils fournis par l'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 de l'État membre en question. Ces juridictions devraient disposer d'une pleine compétence, et notamment de celle d'examiner toutes les questions de fait et de droit relatives au litige dont elles sont saisies.

(87)Lorsqu'une personne concernée estime que les droits que lui confère la présente directive ne sont pas respectés, elle devrait avoir le droit de mandater un organisme qui œuvre à la protection des droits et intérêts des personnes concernées dans le domaine de la protection des données à caractère personnel et qui est constitué conformément au droit d'un État membre, pour qu'il introduise une réclamation en son nom auprès d'une autorité de contrôle et pour qu'il exerce le droit à un recours juridictionnel. Le droit de représentation des personnes concernées ne devrait pas porter atteinte au droit procédural d'un État membre qui peut prévoir que les personnes concernées doivent être obligatoirement représentées devant les juridictions nationales par un avocat au sens de la directive 77/249/CEE du Conseil [(10)].

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

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

(90)Afin d'assurer des conditions uniformes d'exécution de la présente directive, il convient de conférer des compétences d'exécution à la Commission en ce qui concerne le niveau adéquat de protection offert par un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale, ainsi que la forme et les procédures de l'assistance mutuelle et les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle et entre les autorités de contrôle et le comité. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil (11).

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

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

(93)Étant donné que les objectifs de la présente directive, à savoir protéger les libertés et les droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel, et garantir le libre échange des données à caractère personnel par les autorités compétentes au sein de l'Union, ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent, 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 tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(94)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 réglementent 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 devraient demeurer inchangées, tels que, par exemple, les dispositions particulières relatives à la protection des données à caractère personnel appliquées en vertu de la décision 2008/615/JAI (12) ou l'article 23 de la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (13). Étant donné que l'article 8 de la Charte et l'article 16 du traité sur le fonctionnement de l'Union européenne exigent que le droit fondamental à la protection des données à caractère personnel soit garanti de manière homogène dans l'ensemble de l'Union, la Commission devrait évaluer la situation en ce qui concerne la relation entre la présente directive et les actes adoptés avant la date d'adoption de la présente directive qui réglementent le traitement des données à caractère personnel entre États membres ou l'accès d'autorités désignées des États membres aux systèmes d'information créés en vertu des traités, afin d'apprécier la nécessité de mettre ces dispositions particulières en conformité avec la présente directive. Le cas échéant, la Commission devrait faire des propositions en

vue d'assurer la cohérence des règles juridiques relatives au traitement des données à caractère personnel.

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

(96) Les États membres devraient disposer d'un délai maximal de deux ans à compter de la date d'entrée en vigueur de la présente directive pour sa transposition. Les traitements déjà en cours à cette date devraient être mis en conformité avec la présente directive dans un délai de deux ans après son entrée en vigueur. Toutefois, lorsque ces traitements ont lieu en conformité avec le droit de l'Union applicable avant la date d'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 opérations de traitement déjà en cours à ladite date, étant donné que ces exigences, de par leur nature même, doivent être satisfaites avant le traitement. Lorsque les États membres recourent au délai de mise en œuvre plus long, venant à expiration sept ans après la date d'entrée en vigueur de la présente directive, pour se conformer aux obligations en matière de journalisation pour les systèmes de traitement automatisé mis en place avant cette date, le responsable du traitement ou le sous-traitant devrait s'être doté des moyens effectifs de démontrer la licéité du traitement des données, de pratiquer l'autocontrôle et de garantir l'intégrité et la sécurité des données, tels que des journaux ou d'autres formes de registres.

(97) La présente directive s'entend sans préjudice des règles 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 [(14)].

(98) Il y a dès lors lieu d'abroger la décision-cadre 2008/977/JAI.

(99) Conformément à l'article 6 *bis* du protocole n° 21 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 et l'Irlande ne sont pas liés 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.

(100) Conformément aux articles 2 et 2 *bis* du protocole n° 22 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 décide, 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.

(101)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 [15].

(102)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 [16].

(103)En ce qui concerne le Liechtenstein, la présente directive constitue un développement des dispositions de l'acquis de Schengen au sens du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen [17].

(104)La présente directive respecte les droits fondamentaux et observe les principes reconnus par la Charte, tels qu'ils sont consacrés par le traité sur le fonctionnement de l'Union européenne, 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 accéder à un tribunal impartial. 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.

(105)Conformément à la déclaration politique commune du 28 septembre 2011 des États membres et de la Commission 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 mesures nationales de transposition. En ce qui concerne la présente directive, le législateur estime que la transmission de ces documents est justifiée.

(106)Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 et a rendu son avis le 7 mars 2012 [18].

(107)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 aux données à caractère personnel, de rectification ou d'effacement de celles-ci et de limitation du traitement dans le cadre de poursuites pénales, et les éventuelles limitations de ces droits, dans leurs règles nationales en matière de procédure pénale,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

Dispositions générales

Article premier

Objet et objectifs

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

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

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

b) veillent à ce que l'échange de données à caractère personnel par les autorités compétentes au sein de l'Union, lorsque cet échange est requis par le droit de l'Union ou le droit d'un État membre, 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.

3. La présente directive n'empêche pas les États membres de prévoir des garanties plus étendues que celles établies dans 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.

Article 2

Champ d'application

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

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

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

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

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

Article 3

Définitions

Aux fins de la présente directive, on entend par:

1. «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs

éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

2. «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de 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, la limitation, l'effacement ou la destruction;

3. «limitation du traitement», le marquage de données à caractère personnel conservées en vue de limiter leur traitement futur;

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

5. «pseudonymisation», le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

6. «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;

7. «autorité compétente»:

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

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

8. «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 de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou le droit d'un État membre;

9. «sous-traitant», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

10. «destinataire», la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non

d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement;

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

12. «données génétiques», les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

13. «données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

14. «données concernant la santé», les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;

15. «autorité de contrôle», une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 41;

16. «organisation internationale», une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.

CHAPITRE II

Principes

Article 4

Principes relatifs au traitement des données à caractère personnel

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

a) traitées de manière licite et loyale;

b) collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités;

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

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

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

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

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

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

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

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

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

Article 5

Délais de conservation et d'examen

Les États membres prévoient que des délais appropriés sont fixés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel. Des règles procédurales garantissent le respect de ces délais.

Article 6

Distinction entre différentes catégories de personnes concernées

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

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

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

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

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

Article 7

Distinction entre les données à caractère personnel et vérification de la qualité des données à caractère personnel

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

2. Les États membres prévoient que les autorités compétentes prennent toutes les mesures raisonnables pour garantir 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, sont ajoutées des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, et de la fiabilité des données à caractère personnel, et de leur niveau de mise à jour.

3. S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 16.

Article 8

Licéité du traitement

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

2. Une disposition du droit d'un État membre qui réglemente le traitement relevant du champ d'application de la présente directive précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement.

Article 9

Conditions spécifiques applicables au traitement

1. Les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées à l'article 1er, paragraphe 1, ne peuvent être traitées à des fins autres que celles énoncées à l'article 1er, paragraphe 1, à moins qu'un tel traitement ne soit autorisé par le droit de l'Union ou le droit d'un État membre. Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.

2. Lorsque les autorités compétentes sont chargées par le droit d'un État membre d'exécuter des missions autres que celles exécutées pour les finalités énoncées à l'article 1er, paragraphe 1, le règlement (UE) 2016/679 s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.

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

4. Les États membres prévoient que l'autorité compétente qui transmet les données n'applique pas aux destinataires dans les autres États membres ou aux services, organes et organismes établis en vertu des chapitres 4 et 5 du titre V du traité sur le fonctionnement de l'Union européenne des conditions en vertu du paragraphe 3 différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État membre dont relève l'autorité compétente qui transmet les données.

Article 10

Traitement 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, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement:

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

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

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

Article 11

Décision individuelle automatisée

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

2. Les décisions visées au paragraphe 1 du présent article ne sont pas fondées sur les catégories particulières de données à caractère personnel visées à l'article 10, à moins que des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée ne soient en place.

3. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 10 est interdit, conformément au droit de l'Union.

CHAPITRE III

Droits de la personne concernée

Article 12

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

1. Les États membres prévoient que le responsable du traitement prend des mesures raisonnables pour fournir toute information visée à l'article 13 et procède à toute communication relative au traitement ayant trait à l'article 11, aux articles 14 à 18 et à l'article 31 à la personne concernée d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par tout moyen approprié, y compris par voie électronique. De manière générale, le responsable du traitement fournit les informations sous la même forme que la demande.

2. Les États membres prévoient que le responsable du traitement facilite l'exercice des droits conférés à la personne concernée par l'article 11 et les articles 14 à 18.

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

4. Les États membres prévoient qu'aucun paiement n'est exigé pour fournir les informations visées à l'article 13 et pour procéder à toute communication et prendre toute mesure au titre de l'article 11, des articles 14 à 18 et de l'article 31. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut:

a) soit exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder à la communication ou prendre les mesures demandées;

b) soit refuser de donner suite à la demande.

Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

5. Lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée à l'article 14 ou 16, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

Article 13

Informations à mettre à la disposition de la personne concernée ou à lui fournir

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;

b) le cas échéant, les coordonnées du délégué à la protection des données;

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

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

e) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel relatives à une personne concernée.

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

a) la base juridique du traitement,

b)la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

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

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

3. Les États membres peuvent adopter des mesures législatives visant à retarder ou limiter la fourniture des informations à la personne concernée en application du paragraphe 2, ou à ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique 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) protéger la sécurité publique;

d) protéger la sécurité nationale;

e) protéger les droits et libertés d'autrui.

4. Les États membres peuvent adopter des mesures législatives afin de déterminer des catégories de traitements susceptibles de relever, dans leur intégralité ou en partie, d'un quelconque des points énumérés au paragraphe 3.

Article 14

Droit d'accès par la personne concernée

Sous réserve de l'article 15, les États membres prévoient que la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations suivantes:

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

b) les catégories de données à caractère personnel concernées;

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

d)lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

e)l'existence du droit de demander au responsable du traitement la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement des données à caractère personnel relatives à la personne concernée;

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

g)la communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source.

Article 15

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 et aussi longtemps qu'une telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique 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) protéger la sécurité publique;

d) protéger la sécurité nationale;

e) protéger les droits et libertés d'autrui.

2. Les États membres peuvent adopter des mesures législatives afin de déterminer des catégories de traitements de données susceptibles de relever, dans leur intégralité ou en partie, des points a) à e) du paragraphe 1.

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

4. Les États membres prévoient que le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition des autorités de contrôle.

Article 16

Droit de rectification ou d'effacement des données à caractère personnel et 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. Compte tenu des finalités du traitement, les États membres prévoient que la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant à cet effet une déclaration complémentaire.

2. Les États membres exigent que le responsable du traitement efface dans les meilleurs délais les données à caractère personnel et accordent à la personne concernée le droit d'obtenir du responsable du traitement l'effacement dans les meilleurs délais de données à caractère personnel la concernant lorsque le traitement constitue une violation des dispositions adoptées en vertu de l'article 4, 8 ou 10 ou lorsque les données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.

3. Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement lorsque:

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

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

Lorsque le traitement est limité en vertu du premier alinéa, point a), le responsable du traitement informe la personne concernée avant de lever la limitation du traitement.

4. 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 à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus. Les États membres peuvent adopter des mesures législatives limitant, en tout ou partie, l'obligation de fournir ces informations, dès lors qu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique 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) protéger la sécurité publique;

d) protéger la sécurité nationale;

e) protéger les droits et libertés d'autrui.

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

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

6. Les États membres prévoient que, lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des paragraphes 1, 2 et 3, le responsable du traitement adresse une notification aux destinataires et que ceux-ci rectifient ou effacent les données à caractère personnel ou limitent le traitement des données à caractère personnel sous leur responsabilité.

Article 17

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

1. Dans les cas visés à l'article 13, paragraphe 3, à l'article 15, paragraphe 3, et à l'article 16, paragraphe 4, les États membres adoptent des mesures afin que les droits de la personne concernée puissent également être exercés par l'intermédiaire de l'autorité de contrôle compétente.

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

3. Lorsque le droit visé au paragraphe 1 est exercé, l'autorité de contrôle informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. L'autorité de contrôle informe également la personne concernée de son droit de former un recours juridictionnel.

Article 18

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

Les États membres peuvent prévoir que les droits visés aux articles 13, 14 et 16 sont exercés conformément au droit d'un État membre 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 et d'une procédure pénale.

CHAPITRE IV

Responsable du traitement et sous-traitant

Section 1

Obligations générales

Article 19

Obligations incombant au responsable du traitement

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

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

Article 20

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

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

2. Les États membres prévoient que le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cette obligation s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont

pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne concernée.

Article 21

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, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect de la présente directive, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées à l'article 13, par voie d'accord entre eux, sauf si et dans la mesure où leurs obligations respectives sont définies par le droit de l'Union ou le droit d'un État membre auquel les responsables du traitement sont soumis. Le point de contact pour les personnes concernées est désigné dans l'accord. Les États membres peuvent préciser lequel des responsables conjoints peut servir de point de contact unique pour que les personnes concernées puissent exercer leurs droits.

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

Article 22

Sous-traitant

1. Les États membres prévoient que le responsable du traitement, lorsqu'un traitement doit être effectué pour son compte, fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences de la présente directive et garantisse la protection des droits de la personne concernée.

2. Les États membres prévoient que le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe 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.

3. Les États membres prévoient que le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement et qui définit 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 et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant:

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

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

c)aide le responsable du traitement, par tout moyen approprié, à veiller au respect des dispositions relatives aux droits de la personne concernée;

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

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

f)respecte les conditions visées aux paragraphes 2 et 3 pour recruter un autre sous-traitant.

4. Le contrat ou l'autre acte juridique visé au paragraphe 3 revêt la forme écrite, y compris la forme électronique.

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

Article 23

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

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

Article 24

Registre des activités de traitement

1. Les États membres prévoient que les responsables du traitement tiennent un registre de toutes les catégories d'activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:

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

b) les finalités du traitement;

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

d)une description des catégories de personnes concernées et des catégories de données à caractère personnel;

e) le cas échéant, le recours au profilage;

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

g)une indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées;

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

i)dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 29, paragraphe 1.

2. Les États membres prévoient que chaque sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant:

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

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

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

d)dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 29, paragraphe 1.

3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite, y compris la forme électronique.

Le responsable du traitement et le sous-traitant mettent ces registres à la disposition de l'autorité de contrôle, sur demande.

Article 25

Journalisation

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

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

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

Article 26

Coopération avec l'autorité de contrôle

Les États membres prévoient que le responsable du traitement et le sous-traitant coopèrent avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions.

Article 27

Analyse d'impact relative à la protection des données

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

2. L'analyse visée au paragraphe 1 contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect de la présente directive, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées.

Article 28

Consultation préalable de l'autorité de contrôle

1. Les États membres prévoient que le responsable du traitement ou le sous-traitant consulte l'autorité de contrôle préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer:

a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 27, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; ou

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

2. Les États membres prévoient que l'autorité de contrôle est consultée dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative qui se rapporte au traitement.

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

4. Les États membres prévoient que le responsable du traitement fournit à l'autorité de contrôle l'analyse d'impact relative à la protection des données en vertu de l'article 27 et, sur demande, toute autre information afin de permettre à l'autorité de contrôle d'apprécier la conformité du traitement et, en particulier, les risques pour la protection des données à caractère personnel de la personne concernée et les garanties qui s'y rapportent.

5. Les États membres prévoient que, lorsque l'autorité de contrôle est d'avis que le traitement prévu, visé au paragraphe 1 du présent article, constituerait une violation des dispositions adoptées en vertu de la présente directive, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournit par écrit, dans un délai maximum de six semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement, et le cas échéant au sous-traitant, et elle peut faire usage des pouvoirs visés à l'article 47. Ce délai peut être prolongé d'un mois, en fonction de la complexité du traitement prévu. L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de toute prorogation dans un délai d'un mois à compter de la réception de la demande de consultation, ainsi que des motifs du retard.

Section 2
Sécurité des données

Article 29

Sécurité du traitement

1. Les États membres prévoient que, compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel visées à l'article 10.

2. En ce qui concerne le traitement automatisé, 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 (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 à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation);

d) empêcher que les systèmes de traitement automatisé 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 ne puissent accéder qu'aux données à caractère personnel 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, 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).

Article 30

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

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

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

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

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

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

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

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

4. Si et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

5. Les États membres prévoient que le responsable du traitement documente toute violation de données à caractère personnel visée au paragraphe 1, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

6. Les États membres prévoient que, lorsque la violation de données à caractère personnel 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.

Article 31

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

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

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et les mesures visées à l'article 30, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

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

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

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

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

5. La communication à la personne concernée visée au paragraphe 1 du présent article peut être retardée, limitée ou omise, sous réserve des conditions et pour les motifs visés à l'article 13, paragraphe 3.

Section 3
Délégué à la protection des données

Article 32

Désignation du délégué à la protection des données

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

2. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à exercer les missions visées à l'article 34.

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 publie les coordonnées du délégué à la protection des données et les communique à l'autorité de contrôle.

Article 33

Fonction du délégué à la protection des données

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

2. Le responsable du traitement aide le délégué à la protection des données à exercer les missions visées à l'article 34 en fournissant les ressources nécessaires pour exercer ces missions ainsi que l'accès aux données à caractère personnel et aux traitements, et lui permettant d'entretenir ses connaissances spécialisées.

Article 34

Missions du délégué à la protection des données

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

a) informer et conseiller le responsable du traitement et les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la présente directive et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;

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

c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 27;

d) coopérer avec l'autorité de contrôle;

e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 28, et mener des consultations, le cas échéant, sur tout autre sujet.

CHAPITRE V

Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales

Article 35

Principes généraux applicables aux transferts de données à caractère personnel

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

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

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

c) 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 conformément à son droit national;

d)la Commission a adopté une décision d'adéquation en application de l'article 36, ou, en l'absence d'une telle décision, des garanties appropriées ont été prévues ou existent en application de l'article 37 ou, en l'absence de décision d'adéquation au titre de l'article 36 et de garanties appropriées conformément à l'article 37, des dérogations pour des situations particulières s'appliquent en vertu de l'article 38; et

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

2. Les États membres prévoient que les transferts effectués sans l'autorisation préalable d'un autre État membre prévue au paragraphe 1, point c), sont 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 retard.

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

Article 36

Transferts sur la base d'une décision d'adéquation

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

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

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

b)l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire

appliquer, y compris par des pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres; et

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

3. La Commission, après avoir évalué le caractère adéquat du niveau de protection, peut constater au moyen d'un acte d'exécution qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers en question, ou une organisation internationale, assure un niveau de protection adéquat au sens du paragraphe 2 du présent article. L'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale. L'acte d'exécution précise son champ d'application territorial et sectoriel et, le cas échéant, nomme la ou des autorités de contrôle visées au paragraphe 2, point b), du présent article. L'acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 58, paragraphe 2.

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

5. Lorsque les informations disponibles révèlent, en particulier à la suite de l'examen visé au paragraphe 3 du présent article, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat au sens du paragraphe 2 du présent article, la Commission abroge, modifie ou suspend, si nécessaire, la décision visée au paragraphe 3 du présent article par voie d'actes d'exécution sans effet rétroactif. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 58, paragraphe 2.

Pour des raisons d'urgence impérieuses dûment justifiées, la Commission adopte des actes d'exécution immédiatement applicables en conformité avec la procédure visée à l'article 58, paragraphe 3.

6. 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.

7. Les États membres prévoient qu'une décision adoptée en vertu du paragraphe 5 est sans préjudice des transferts de données à caractère personnel vers le pays tiers, le territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou à l'organisation internationale en question, effectués en application des articles 37 et 38.

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

Article 37

Transferts moyennant des garanties appropriées

1. En l'absence de décision en vertu de l'article 36, 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 sont fournies dans un instrument juridiquement contraignant; ou

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

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

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

Article 38

Dérogations pour des situations particulières

1. En l'absence de décision d'adéquation en vertu de l'article 36 ou de garanties appropriées en vertu de l'article 37, 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 qu'à condition que le transfert soit nécessaire:

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

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

c)pour prévenir une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers;

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

e)dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les fins énoncées à l'article 1er, paragraphe 1.

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

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

Article 39

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

1. Par dérogation à l'article 35, paragraphe 1, point b), et sans préjudice de tout accord international visé au paragraphe 2 du présent article, le droit de l'Union ou le droit d'un État membre peut prévoir que les autorités compétentes au sens de l'article 3, point 7) a), peuvent, dans certains cas particuliers, transférer des données à caractère personnel directement aux destinataires établis dans des pays tiers, uniquement lorsque les autres dispositions de la présente directive sont respectées et que toutes les conditions ci-après sont remplies:

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

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

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

d)l'autorité qui est compétente aux fins visées à l'article 1er, paragraphe 1, dans le pays tiers est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié;

e)l'autorité compétente qui transfère les données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel ne doivent faire l'objet d'un traitement que par cette dernière, à condition qu'un tel traitement soit nécessaire.

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

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

4. Lorsqu'un transfert est effectué sur la base du paragraphe 1, ce transfert est documenté.

Article 40

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

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

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

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

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

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

CHAPITRE VI

Autorités de contrôle indépendantes

Section 1
Statut d'indépendance

Article 41

Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application de la présente directive, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union (ci-après dénommées «autorité de contrôle»).

2. 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.

3. Les États membres peuvent prévoir qu'une autorité de contrôle instituée au titre du règlement (UE) 2016/679 est l'autorité de contrôle visée dans la présente directive et prend en charge les missions de l'autorité de contrôle devant être instituée en vertu du paragraphe 1 du présent article.

4. Lorsqu'un État membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité visé à l'article 51.

Article 42

Indépendance

1. Chaque État membre prévoit que chaque autorité de contrôle agit en toute indépendance dans l'exercice de ses missions et des pouvoirs dont elle est investie conformément à la présente directive.

2. Les États membres prévoient que, dans l'exercice de leurs missions et de leurs pouvoirs conformément à la présente directive, le ou les membres de leurs autorités 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. Le ou les membres des autorités de contrôle des États membres s'abstiennent de tout acte incompatible avec leurs fonctions et, pendant la durée de leur mandat, n'exercent aucune activité professionnelle incompatible, rémunérée ou non.

4. Chaque État membre veille à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsque celle-ci doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité.

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

6. Chaque État membre veille à ce que chaque autorité de contrôle soit soumise à un contrôle financier qui ne menace pas son indépendance et qu'elle dispose d'un budget annuel public propre, qui peut faire partie du budget global national ou d'une entité fédérée.

Article 43

Conditions générales applicables aux membres de l'autorité de contrôle

1. Les États membres prévoient que chacun des membres de leurs autorités de contrôle est nommé selon une procédure transparente par:

— leur parlement,

— leur gouvernement,

— leur chef d'État, ou

—un organisme indépendant chargé de procéder à la nomination en vertu du droit de l'État membre.

2. Chaque membre a les qualifications, l'expérience et les compétences nécessaires, en particulier dans le domaine de la protection des données à caractère personnel, pour l'exercice de leurs fonctions et de leurs pouvoirs.

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

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

Article 44

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

1. Chaque État membre prévoit, par la loi, tous les éléments suivants:

a) la création de chaque autorité de contrôle;

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

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

d)la durée du mandat du ou des membres de chaque autorité de contrôle, qui ne peut être inférieure à quatre ans, sauf pour la première nomination après le 6 mai 2016, dont une partie 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 ou des membres de chaque autorité de contrôle et, si c'est le cas, le nombre de mandats;

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

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

Section 2

Compétence, missions et pouvoirs

Article 45

Compétence

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

2. Chaque État membre prévoit que chaque autorité de contrôle n'est pas compétente pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle. Les États membres peuvent prévoir que leur autorité de contrôle n'est pas compétente pour contrôler les opérations de traitement effectuées par d'autres autorités judiciaires indépendantes lorsqu'elles agissent dans l'exercice de leur fonction juridictionnelle.

Article 46

Missions

1. Chaque État membre prévoit que, sur son territoire, chaque autorité de contrôle:

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

b)favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement;

c)conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement;

d)encourage la sensibilisation des responsables du traitement et des sous-traitants aux obligations qui leur incombent en vertu de la présente directive;

e)fournit, sur demande, à toute personne concernée, des informations sur l'exercice de ses droits découlant de la présente directive et, le cas échéant, coopère à cette fin avec les autorités de contrôle d'autres États membres;

f)traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association conformément à l'article 55, enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire;

g)vérifie la licéité du traitement en vertu de l'article 17, et informe la personne concernée dans un délai raisonnable de l'issue de la vérification, conformément au paragraphe 3 dudit article, ou des motifs ayant empêché sa réalisation;

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

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

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

k) fournit des conseils sur les opérations de traitement visées à l'article 28; et

l) contribue aux activités du comité.

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

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

4. Lorsqu'une demande est manifestement infondée ou excessive, en raison, notamment, de son caractère répétitif, l'autorité de contrôle peut exiger le paiement de frais raisonnables basés sur ses coûts administratifs ou refuser de donner suite à la demande. Il incombe à l'autorité de contrôle de démontrer le caractère manifestement infondé ou excessif de la demande.

Article 47

Pouvoirs

1. Chaque État membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs d'enquête effectifs. Ces pouvoirs comprennent au moins celui 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.

2. Chaque État membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs effectifs en matière d'adoption de mesures correctrices, tels que, par exemple:

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

b) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions adoptées en vertu de la présente directive, le cas échéant, de manière spécifique et dans un délai déterminé, en particulier en ordonnant la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application de l'article 16;

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

3. Chaque État membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs consultatifs effectifs pour conseiller le responsable du traitement conformément à la procédure de consultation préalable visée à l'article 28 et d'émettre, de sa propre initiative ou sur demande, des avis à l'attention de son parlement national et de son gouvernement ou, conformément à son droit national, d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel.

4. 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 juridictionnel effectif et à une procédure régulière, prévues par le droit de l'Union et le droit de l'État membre conformément à la Charte.

5. Chaque État membre prévoit, par la loi, que chaque autorité de contrôle a le pouvoir de porter les violations des dispositions adoptées en vertu de la présente directive à la connaissance des autorités judiciaires 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 48

Signalement des violations

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

Article 49

Rapports d'activité

Chaque autorité de contrôle établit un rapport annuel sur ses activités, qui peut comprendre une liste des types de violations notifiées et des types de sanctions imposées. Les rapports sont transmis au parlement national, au gouvernement et à d'autres autorités désignées par le droit de l'État membre. Ils sont mis à la disposition du public, de la Commission et du comité.

CHAPITRE VII

Coopération

Article 50

Assistance mutuelle

1. Chaque État membre prévoit que leurs autorités de contrôle se communiquent les informations utiles et se prêtent mutuellement assistance en vue de mettre en œuvre et d'appliquer la présente directive de façon cohérente, et met en place des mesures pour coopérer efficacement. L'assistance mutuelle concerne notamment les demandes d'information et les mesures de contrôle, telles que les demandes de consultation, les inspections et les enquêtes.

2. Chaque État membre prévoit que chaque autorité de contrôle prend toutes les mesures appropriées requises pour répondre à la demande d'une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande. De telles mesures peuvent comprendre notamment la transmission d'informations utiles sur la conduite d'une enquête.

3. Les demandes d'assistance contiennent toutes les informations nécessaires, notamment la finalité et les motifs de la demande. Les informations échangées ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

4. Une autorité de contrôle saisie d'une demande ne peut refuser d'y satisfaire, sauf si:

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

b) satisfaire à la demande constituerait une violation de la présente directive ou du droit de l'Union ou du droit de l'État membre auquel l'autorité de contrôle qui a reçu la demande est soumise.

5. 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. L'autorité de contrôle requise donne les motifs de tout refus de satisfaire à une demande en application du paragraphe 4.

6. Les autorités de contrôle requises communiquent, en règle générale, par voie électronique et au moyen d'un formulaire type, les informations demandées par d'autres autorités de contrôle.

7. Les autorités de contrôle requises ne perçoivent pas de frais pour une mesure qu'elles prennent à la suite d'une demande d'assistance mutuelle. Les autorités de contrôle peuvent convenir de règles concernant l'octroi de dédommagements entre elles pour des dépenses spécifiques résultant de la fourniture d'une assistance mutuelle dans des circonstances exceptionnelles.

8. La Commission peut, par voie d'actes d'exécution, préciser la forme et les procédures de l'assistance mutuelle visée au présent article, ainsi que les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle et entre les autorités de contrôle et le comité. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 58, paragraphe 2.

Article 51

Missions du comité

1. Le comité institué par le règlement (UE) 2016/679 exerce les missions ci-après en ce qui concerne les activités de traitement relevant du champ d'application de la présente directive:

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

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

c) élaborer, à l'intention des autorités de contrôle, des lignes directrices concernant l'application des mesures visées à l'article 47, paragraphes 1 et 3;

d) publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point b) du présent alinéa, en vue d'établir les violations de données à caractère personnel et de déterminer les meilleurs délais visés à l'article 30, paragraphes 1 et 2, et de préciser les circonstances particulières dans lesquelles un responsable du traitement ou un sous-traitant est tenu de notifier la violation des données à caractère personnel;

e) publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point b) du présent alinéa concernant les circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, comme le prévoit l'article 31, paragraphe 1;

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

g) rendre à la Commission un avis en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, y compris concernant l'évaluation visant à déterminer si ce pays tiers, ce territoire, ce secteur déterminé ou cette organisation internationale n'assure plus un niveau adéquat de protection;

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

i) 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 avec des organisations internationales;

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

En ce qui concerne le point g) du premier alinéa, la Commission fournit au comité tous les documents nécessaires, y compris la correspondance avec le gouvernement du pays tiers, le territoire ou le secteur déterminé dans ce pays tiers, ou avec l'organisation internationale.

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

3. Le comité transmet ses avis, lignes directrices, recommandations et bonnes pratiques à la Commission et au comité visé à l'article 58, paragraphe 1, et les publie.

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

CHAPITRE VIII

Voies de recours, responsabilité et sanctions

Article 52

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 constitue une violation des dispositions adoptées en vertu de la présente directive.

2. Les États membres prévoit que, si la réclamation n'est pas introduite auprès de l'autorité de contrôle compétente au titre de l'article 45, paragraphe 1, l'autorité de contrôle auprès de laquelle la réclamation a été introduite la transmet dans les meilleurs délais à l'autorité de contrôle compétente. La personne concernée est informée de cette transmission.

3. 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.

4. 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 53.

Article 53

Droit à un recours juridictionnel effectif contre une autorité de contrôle

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

2. Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit de former un recours juridictionnel effectif lorsque l'autorité de contrôle qui est compétente en vertu de l'article 45, paragraphe 1, ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite au titre de l'article 52.

3. Les États membres disposent 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 54

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 d'introduire une réclamation auprès d'une autorité de contrôle en vertu de l'article 52, une personne concernée a droit à un recours juridictionnel effectif lorsqu'elle considère que ses droits prévus dans les dispositions adoptées en vertu de la présente directive ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation desdites dispositions.

Article 55

Représentation des personnes concernées

Les États membres prévoient, conformément à leur droit procédural, que la personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel la concernant, pour qu'il introduise une réclamation en son nom et exerce en son nom les droits visés aux articles 52, 53 et 54.

Article 56

Droit à réparation

Les États membres prévoient que toute personne ayant subi un dommage matériel ou un préjudice moral du fait d'une opération de traitement illicite ou de toute action qui constitue une violation des dispositions nationales adoptées en vertu de la présente directive a le droit d'obtenir du responsable du traitement, ou de toute autre autorité compétente en vertu du droit d'un État membre, réparation du préjudice subi.

Article 57

Sanctions

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

CHAPITRE IX

Actes d'exécution

Article 58

Comité

1. La Commission est assistée par le comité institué par l'article 93 du règlement (UE) 2016/679. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

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

3. Lorsqu'il est fait référence au présent paragraphe, l'article 8 du règlement (UE) nº 182/2011 s'applique, en liaison avec son article 5.

CHAPITRE X

Dispositions finales

Article 59

Abrogation de la décision-cadre 2008/977/JAI

1. La décision-cadre 2008/977/JAI est abrogée à compter du 6 mai 2018.

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

Article 60

Actes juridiques de l'Union déjà en vigueur

Les dispositions spécifiques relatives à la protection des données à caractère personnel figurant dans des actes juridiques de l'Union qui sont entrés en vigueur le 6 mai 2016 ou avant cette date dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, qui réglementent le traitement entre États membres et l'accès des autorités nationales désignées des États membres aux systèmes d'information créés en vertu des traités, dans le cadre de la présente directive, demeurent inchangées.

Article 61

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 le 6 mai 2016 et qui respectent le droit de l'Union tel qu'il est applicable avant cette date restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation.

Article 62

Rapports de la Commission

1. Au plus tard le 6 mai 2022, et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen de la présente directive. Ces rapports sont publiés.

2. Dans le cadre de ces évaluations et réexamens visés au paragraphe 1, la Commission examine, en particulier, l'application et le fonctionnement du chapitre V sur le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, en accordant une attention particulière aux décisions adoptées en vertu de l'article 36, paragraphe 3, et de l'article 39.

3. Aux fins des paragraphes 1 et 2, la Commission peut demander des informations aux États membres et aux autorités de contrôle.

4. Lorsqu'elle procède aux évaluations et réexamens visés aux paragraphes 1 et 2, la Commission tient compte des positions et des conclusions du Parlement européen, du Conseil ainsi que d'autres organismes ou sources pertinents.

5. La Commission présente, si nécessaire, des propositions législatives visant à modifier la présente directive, en particulier en tenant compte des évolutions en matière de technologie de l'information et de l'état d'avancement de la société de l'information.

6. Au plus tard le 6 mai 2019, la Commission réexamine d'autres actes juridiques adoptés par l'Union qui réglementent le traitement par les autorités compétentes aux fins énoncées à l'article 1er, paragraphe 1, y compris ceux qui sont visés à l'article 60, 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.

Article 63

Transposition

1. Les États membres adoptent et publient, au plus tard le 6 mai 2018, 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 6 mai 2018.

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. Par dérogation au paragraphe 1, un État membre peut prévoir que, à titre exceptionnel, lorsque cela exige des efforts disproportionnés, les systèmes de traitement automatisé installés avant le 6 mai 2016 sont mis en conformité avec l'article 25, paragraphe 1, au plus tard le 6 mai 2023.

3. Par dérogation aux paragraphes 1 et 2 du présent article, un État membre peut, dans des circonstances exceptionnelles, mettre un système donné de traitement automatisé visé au paragraphe 2 du présent article, en conformité avec l'article 25, paragraphe 1, dans un délai déterminé après le délai visé au paragraphe 2 du présent article, lorsque, à défaut de cela, de graves difficultés se poseraient pour le fonctionnement du système de traitement automatisé en question. L'État membre concerné notifie à la Commission les raisons de ces graves difficultés et les motifs justifiant le délai déterminé de mise en conformité du système donné de traitement automatisé avec l'article 25, paragraphe 1. Le délai déterminé n'est en aucun cas fixé au-delà du 6 mai 2026.

4. 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 64

Entrée en vigueur

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

Article 65

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le 27 avril 2016.

Par le Parlement européen

Le président

M. SCHULZ

Par le Conseil

Le président

J.A. HENNIS-PLASSCHAERT